丘成桐主编
数学翻译丛书

Number Theory

An approach through history from Hammurapi to Legendre

[法] André Weil 著　胥鸣伟 译　王元 校

数论

——从汉穆拉比到勒让德的历史导引



高等教育出版社
HIGHER EDUCATION PRESS

丘成桐主编
数学翻译丛书

数论

——从汉穆拉比到勒让德的历史导引

Shulun

[法] André Weil 著　胥鸣伟 译　王元 校

17 幅插图

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING
International Press

图字：01–2010–1384 号

Translation from the English language edition:
Number Theory by André Weil

图书在版编目 (CIP) 数据

数论: 从汉穆拉比到勒让德的历史导引 / (法) 韦伊 (Weil, A.) 著; 胥鸣伟译. — 北京: 高等教育出版社, 2010.4
(数学翻译丛书 / 丘成桐主编)
书名原文: Number Theory: An approach through history from Hammurapi to Legendre
ISBN 978-7-04-029213-8

I. ①数… II. ①韦…②胥… III. ①数论–数学史 IV. ①O156-09

中国版本图书馆 CIP 数据核字 (2010) 第 045672 号

策划编辑	赵天夫	**责任编辑**	李　鹏	**封面设计**	王凌波
责任绘图	黄建英	**责任印制**	朱学忠		

出版发行	高等教育出版社	**购书热线**	010–58581118
社　　址	北京市西城区德外大街 4 号	**免费咨询**	400–810–0598
邮政编码	100120	**网　　址**	http://www.hep.edu.cn
总　　机	010–58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京信彩瑞禾印刷厂	**畅想教育**	http://www.widedu.com
开　　本	787 × 1092　1/16	**版　　次**	2010 年 4 月第 1 版
印　　张	18.25	**印　　次**	2010 年 4 月第 1 次印刷
字　　数	320 000	**定　　价**	56.00 元

本书如有缺页、倒页、脱页等质量问题, 请到所购图书销售部门联系调换。

物 料 号　29213–00

《数学翻译丛书》序

改革开放以后, 国内大学逐渐与国外的大学增加交流. 无论到国外留学或邀请外地学者到中国访问的学者每年都有增长, 对中国的科学现代化都大有帮助. 但是在翻译外国文献方面的工作尚不能算多. 基本上所有中国的教科书都还是由本国教授撰写, 有些已经比较陈旧, 追不上时代了. 很多国家, 例如俄罗斯、日本等, 都大量翻译外文书本来增长本国国民的阅读内容, 对数学的研究都大有裨益. 高等教育出版社和海外的国际出版社有鉴及此, 开始计划做有系统的翻译, 由王元院士领导, 北京的晨兴数学中心和杭州的浙江大学数学科学研究中心共同组织数学教授进行这个工作. 参与的教授很多, 有杨乐院士, 刘克峰教授等等. 我们希望这套翻译书能够使我们的大学生有更多的角度来看数学, 丰富他们的知识. 海外的出版公司如美国数学会等多有帮助, 我们谨此鸣谢.

丘成桐 (Shing-Tung Yau)

2005 年 1 月

前　言

数论, 一个有关整数性质的深奥专业.
——《时代》, 1983 年 4 月 4 日.

本书所考察的内容涵盖了从一块古巴比伦的泥板到勒让德 (Legendre) 1798 年的《论数论》发表这一漫长的时期, 而其中的这块泥板则可远远地追溯到汉穆拉比王朝[*1] (Hammurapi) 的年代. 大体上, 书的内容截止在 1801 年高斯的《算术研究》发表之前, 但它也包含了关于勒让德以后生涯的一段情节, 从而不可避免地要涉及高斯和他的继承者们的一些发现.

数论, 或者如一些情有独钟的人所称做的算术, 直到最近以来, 一直都以它的献身者们的质量而非数量彰显于世; 或许在所能激发出的热情方面它也是独一无二的, 这种热情雄辩地表现在诸如欧拉 (Euler)、高斯 (Gauss)、艾森斯坦 (Eisenstein)、希尔伯特 (Hilbert) 的许多言辞之中. 因此, 虽然这本书包含了三十六个世纪的一些工作, 但它的绝大部分内容都在于对四位数学家, 即费马 (Fermat)、欧拉、拉格朗日 (Lagrange)、勒让德的成就的细节研讨和解说上. 他们是现代数论的奠基人, 而高斯的伟大之处则在于他使先辈们开创的东西趋于完善, 这等同于他揭开了这门学科在历史上的一个新纪元.

我们的任务是要尽可能地把读者带进我们的这些作者们的制作间, 观察他们的工作状态, 分享他们的成功, 并感受他们的失败. 所幸的是, 这并不需要对

[*1] ? — 公元前 1750 年, 这是古巴比伦王国国王 (公元前 1792—前1750) 的名字, 他在位期间武力统一了美索不达米亚地区, 实行中央集权统治, 颁布了《汉穆拉比法典》. —— 译注; 后文中我们总在译注序号上加以 *, 以与本书原注区分.

于档案材料和故纸堆的任何钻研. 由于所引用的资料将受到验证, 几乎所有在本书中提及的数学家都有他们完整的著作, 他们尚存的通信已被很好地编辑出版. 我的运气也颇好, 能够参阅在高等研究院中的罗森瓦尔德珍本收藏处的一些人的原版资料, 他们是韦达 (Viète)、巴歇 (Bachet)、费马、沃利斯 (Wallis) 和勒让德.

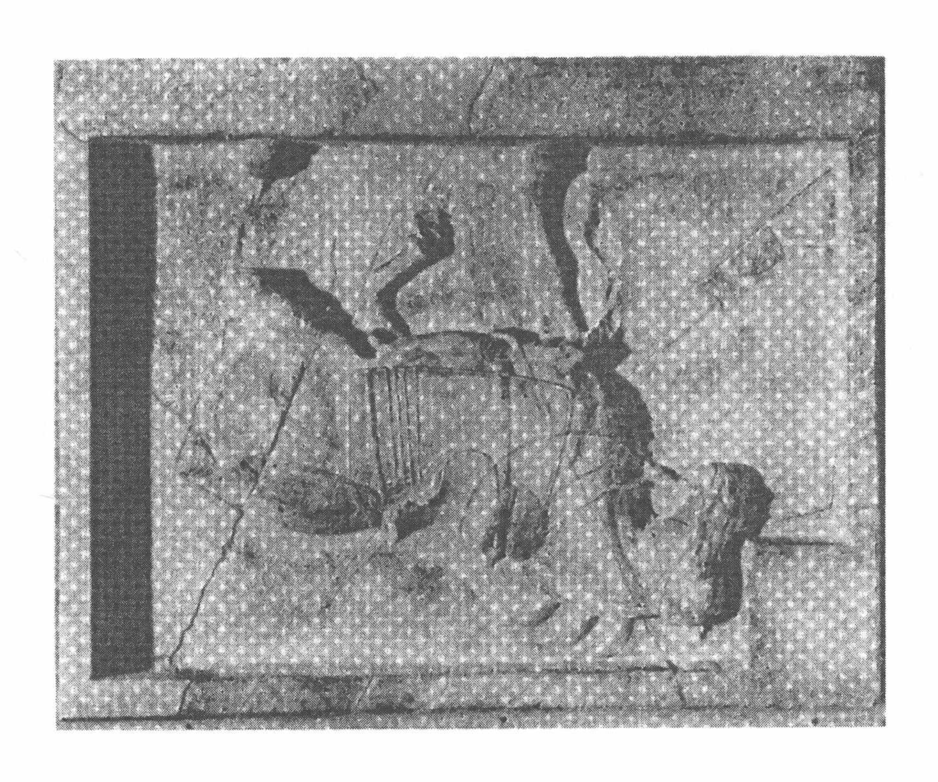
彻底尊重历史是本书所遵循的方法; 不要求读者有专门的知识. 我的热切愿望是, 至少有一些读者能体会到, 他们若依照本书中那条重走的历史路线而将数论作为起点, 这是可行的. 一些适当的背景知识可以从我的《数论初步 (*Number theory for beginners*)》得到 (顺便提一下: 这本书的内容几乎完全取自欧拉), 或者还有 (在一个更高的水平上) J.-P. 塞尔 (Serre)的《算术教程 (*Cours d'Arithmétique*)》的第一章. 更详细的背景信息连同一些补充资料 (并非具严格的史料性质) 可以在第二、三、四章后面的附录中找到.

我, 还有读者, 应该衷心感谢我的朋友陈省身, 他用他漂亮的书法使我们的卷首页增色. 还要感谢宾州大学 (University of Pennsylvania) 的大学博物馆允许我们复制他们藏品中的唐朝六骏之一的照片; 感谢诺伊格鲍尔 (O. Neugebauer) 给了我们泥板 PLIMPTON 322 的照片; 还要感谢巴黎的科学院档案馆, 给了我们有 Delpech 雕画的拉格朗日像的照片. 最后, 我愿表达我对波士顿的 Birkhäuser Verlag 的谢意, 特别是对 Klaus Peters 及其合作团队的谢意, 他们对此项目具有强烈的兴趣, 不止一次地伸出援手, 并使用了他们高超的技术能力保证了本书的出版.

1983 年 4 月 15 日于普林斯顿

老馬識途

陳省身題



缩写、基本参考文献以及记号

Arch. = ARCHIMEDES, Opera omnia cum commentariis Eutocii, it.ed. J. L. Heiberg, Teubner, 3 vol., 1910—1915.

D. Bern. = Die Werke von DANIEL BERNOULLI, ed.D. Speiser, Bd. 2, Birkhäuser 1982.

J.Bern. = Johannis BERNOULLI ... Opera Omnia ... Lausannae et Genevae, sumptibus Marci Michaelis Bousquet et sociorum, 4 vol., 1742—1743.

Col. = H. T. COLEBROOKE, Algebra with arithmetic and mensuration. From the sanscrit of Brahmegupta and Bháscara, London 1817 (Reprint, 1972).

Corr. = Correspondance mathématique et physique de quelques célèbres géomètres du XVIII[ème] siècle ... publiée ... par P.-H. Fuss, St.-Pétersbourg, 2 vol., 1843 (reprint, Johnson Reprint Corp., 1968).

Desc. = Œuvres de DESCARTES, pub. par Charles Adam et Paul Tannery, Paris, 11 vol., 1897—1909.

Dioph. = DIOPHANTI Alexandrini Opera omnia cum graecis commentariis, ed. Paulus Tannery, Teubner, 2 vol. 1893—1895.

Dir. = G. Lejeune DIRICHLET's Werke, herausg. v. L. Kronecker und L. Fuchs, Berlin, 2 vol., 1889—97.

Disq. = Disquisitiones arithmeticae, auctore D. Carolo Friderico GAUSS, Lipsiae 1801 (= vol. I of Gauss, Werke, Göttingen 1870).

Eucl. = EUCLIDIS Elementa, ed. I. L. Heiberg, Lipsiae, Teubner, 4 vol., 1883—

1885 (and: Post I. L. Heiberg ed. E. S. Stamatis, Teubner, 4 vol., 1969—1973).

Eu. = Leonhardi EULERI Opera omnia, sub ausp. Soc. scient. Nat. Helv .... Series I–IV A, 1911—).

Fag. = Opere Matematiche del Marchese Giulio Carlo de' Toschi di FAGNANO, pubbl ....dai Soci V. Volterra, G. Loria, D. Gamboli, 3 vol., 1911—1913.

Fe. = Œuvres de Fermat, pub. par ...Paul Tannery et Charles Henry, Paris, 4 vol., 1891—1912 (+ Supplément, pub. par M. C. de Waard, 1 vol. 1922).

Gal. = Le Opere di GALILEO Galilei, Edizione Nazionale, Firenze, G. Barbera, 20 vol., 1890—1909.

Gau. = Carl Friedrich GAUSS, Werke, Göttingen, 12 vol., 1870—1929.

Huy. = Œuvres complètes de Christian HUYGENS, pub. par la Soc. Holl. des Sc., La Haye, Martinus Nijhoff, 22 vol., 1888—1950.

Jac. = C. G. J. JACOBI's Gesammelte Werke, herausg. v. K. Weierstrass, Berlin, 7 vol., 1881—1891.

JEH. = J. E. Hofmann, Neues über FERMATs zahlentheoretische Herausforderungen von 1657, Abh. d. preuss. Akad. d. Wiss. 1943—1944. Nr. 9, pp. 41—47.

Lag. = Œuvres de LAGRANGE, pub. par M. J.-A. Serret et M. Gaston Darboux, Paris, 14 vol., 1867—1892.

Leib. = LEIBNIZens mathematische Schriften, herausg. von C. I. Gerhardt, Zweite Abtheilung, die mathematischen Abhandlungen Leibnizens enthaltend, Halle, 3 vol., 1858—1863.

Leon. = Scritti di LEONARDO PISANO, matematico del Secolo decimoterzo, pubbl. da Baldassare Boncompagni, Roma, 2 vol., 1857—1862.

LVE. = LEONARD DE PISE, Le livre des nombres carrés, traduit ...par P. Ver Eecke, Desclée de Brouwer et Cie, Bruges 1952 (French translation of *Leon.* II. 253—283).

Mers. = Correspondance du P. Marin MERSENNE, Religieux Minime, Pub. par Mme paul Tannery et Cornélis de Waard, Paris, 14 vol., 1955—1980.

New. = The mathematical papers of Isaac NEWTON, ed. by D. T. Whiteside, Cambridge University Press, 8 vol., 1967—1981.

PkU. = Leonhard EULER, Pis'ma k učënym, edd, T. N. Klado, Ju. Ch. Kopelevič, T. A. Lukin (red. V. I. Smirnov), Moskva-Leningrad 1963.

Viète, *Op.* = Francisci VIETAE Opera Mathematica ...Operâ atque studio Francisci à Schooten Leydensis, Matheseos Professoris, Lugduni Batavorum, ex offici-nâ Bonaventurae et Abrahami Eizeviriorum, 1646 (reprint Georg Holms

Verlag 1970).

Wal. = Johannis WALLIS S. T. D., Geometriae Professoris in Celeberrima Academia Oxoniensi, Opera Mathematica: (I) Volumen Primum, Oxoniae, e Theatro Sheldoniano 1695; (II) De Algebra Tractatus Historicus et Practicus, Anno 1685 anglice editus, nunc auctus latine ... Operum Mathematicorum Volumen alterum, Oxoniae ... 1693.

(请看书后部分的补充文献)

文献及日期的说明

对于前面那些著作的参考绝大部分都是以显示卷数 (如有必要) 以及页数来给出. 例如: *Fe.*II,194 表示费马的《*Œuvres*》(在标准的 Tannery-Henry 版本), 第二卷, 194 页.

例外的是, 参考欧几里得和丢番图时是由显示“书”以及命题, 问题给出. 例如: *Eucl.*VII,2 表示欧几里得的 (标准的 Heiberg 版本)书 VII, 命题 2; 类似的, *Dioph.*V,11 表示丢番图的 (Tannery 版本) 书 V, 问题 11. 在丢番图的情形, 有时会发现需要包含 1621 年的巴歇 (Bachet) 版本的编号 (或者等于是在 S.de Fermat 1670 年的版本; 参看文献索引); 因此表示: *Dioph.*V,11=*Dioph.*V,14_b 的意思是丢番图的书 V, 问题 11 (Tannery 版本) 被编为 Bachet 版本的 14.

在对费马和欧拉著作的叙述中日期特别重要 (第二章, 第三章). 在信件的情形一般不会发生问题; 在旧历法 (Julian 历) 和新历法 (Gregorian 历) 之间的差别是很小的, 绝大多数都忽略了. 至于欧拉, 有必要要一个更加精致的系统, 对于他的每篇文章值得标明它在欧拉著述 (参看文献) 的 G.Eneström 分类目录中的编号以及它大体的写作日期. 譬如, *Eu.*I-2,531–555=E271;1758 表示欧拉的论文, Eneström 编号的 no. 271, 系列 I 的第 2 卷, 531 到 555 页, 被认为是 1758 年写的; 当仅参考一篇文章的一部分时, 它这样给出: *Eu.*I-20,81 于 E252 中;1752. 该日期是由 Eneström 给出的 (或者是提交给彼得堡或柏林科学院的日期), 除非欧拉较早已由欧拉的通信表明了日期. 参看系列 IV A 的卷 1 可由以下数字给出: *Eu.*IV A-1, no.1887; 它意思是那一卷编号为 1887 的信件. 这里所说的这个系列是现存的欧拉的通信资料库.

补充的参考资料可在本书最后面的文献目录中找到.

记号

通篇使用了传统的代数记号. 由于到十七世纪后期前还不能说已经充分建

立了这些记号, 在叙述较早期作者的工作 (包括费马, 他使用韦达的记号) 时这样做与当时的时代特征不相符. 但从欧拉以后, 我们的记号则通常与原作者的相符合了, 不过需要除去同余式的记号, 因为这只能追溯到高斯那时, 然而我们为了使用方便的缩写, 通篇都采用了它. 回忆一下, "模" m 的 "同余式"

$$a \equiv b \pmod{m}$$

表示 $a-b$ 是 m 的一个倍数. 因此一个整数 a 是模 m 的 "二次剩余"是指如果有一个 b 使得 $a \equiv b^2 \pmod{m}$, 否则就是一个 "二次非剩余"; 它是一个 n 次剩余是说如果有一个 b 使得 $a \equiv b^n \pmod{m}$.

也是出于简便的原因, 有时也采用了矩阵的记号 (在第三章 §13 以及第四章的附录 III); $\mathbb{Z}$ 用来表示所有整数 (正, 负, 及 0) 的 "环"; $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 分别代表由所有有理数, 所有实数, 所有 "虚数" (或 "复数") $a+b\sqrt{-1}$ 组成的 "域" (其中 a, b 为实数); 当 p 为任意素数时, $\mathbb{F}_p$ 为 p 个元构成的 "域", 它们是模 p 的同余类. 如果 θ 是个 "二次无理数", 实际是 $\sqrt{N}$, 其中 N 是个非平方的整数, 或者 θ 为 "三次单位根" $\dfrac{-1+\sqrt{-3}}{2}$, 则 $\mathbb{Z}[\theta]$ 是个由所有 $a+b\theta$ 元组成的 "环", 其中 a 和 b 为整数, 而 $\mathbb{Q}(\theta)$ 是由 $r+s\theta$ 构成的 "域", 其中 r 和 s 为有理数.

为了打字方便, 勒让德符号

$$\left(\frac{n}{p}\right)$$

(总是被勒让德、狄利克雷及大多数经典作者所使用) 经常被打印成 (n/p). 它的定义是, 只要 p 是个素数, 而 n 是与 p 互素的整数, 那么当 n 是个模 p 的二次剩余时, 它为 $+1$, 否则为 -1.

目　录

插图目录

第一章　原史时期的数论

§1.1　引子

按照雅可比 (Jacobi) 的说法, 椭圆函数的理论诞生于 1751 年 12 月 23 日与 1752 年 1 月 27 日之间. 在前面那个日子里, 柏林科学院将刚从作者那里收到的两卷 1750 年在佩扎罗出版的《数学作品集 (*Produzioni Matematiche*)》交给了欧拉; 作者是意大利侯爵法尼亚诺*1(Fagnano). 欧拉被要求审阅该书并起草一封适当的答谢信. 而在后面的那个日子里, 欧拉明确谈及了法尼亚诺关于双纽线 (lemniscate) 的工作, 并向科学院宣读了他一系列文章中的第一篇, 这些文章最终以完全一般的形式证明了椭圆积分的加法与乘法定理.

人们也可以类似地定出现代数论的诞辰; 然而这有点像酒神巴克斯 (Bacchus) 那样, 似乎要出生两次了*2. 它的第一个生日必定在 1621 年到 1636 年中的某天, 很可能更靠近后面的日期. 在 1621 年, 丢番图*3(Diophantus)的希腊文文本连同一份适用的拉丁文译文及一个范围广泛的评述经由巴歇出版了. 不知道费马是在什么时候得到了该书的一个复本的 (毫无疑问, 这就是他后来在其边白上草草写下一些他最好的发现的那本), 也不知道他是什么时候开始读这本

*1 1682—1766, 专注于椭圆函数及双纽线等弧长的计算.

*2 罗马酒神. 按罗马宗教中所说, 他是先从西姆莱女神腹中取出, 后又被放进朱庇特主神腿中三月.

*3 对其生平知之甚少, 活跃于公元 250 年左右的亚历山大, 主要著述有《算术》、《多角数》等. 本书中作者使用的丢番图一词有时表示人, 大部分则表示了他的著述, 没有严格区分, 请读者留意.

书的, 我们从他的通信中得知, 在 1636 年他不但已经仔细阅读了它, 而且也已经发展出了对与此书相关的各类课题的他自己的想法.

从此以后, "数", 即数论再没有离开费马的主要兴趣一步, 然而他为他钟爱的学科来赢取朋友的勇敢努力, 总的来说, 并没有获得成功. 年轻的惠更斯*4 (Huygens) 对沃利斯*5评说道:"我们并不缺少值得花我们时间的更好课题" (*Huy.* II,211=*Fe.*IV,121). 费马曾经抱有全身心投入到写出一本完整的数论书的想法 (*Fe.*I,305). 在一个场合他试图劝说帕斯卡*6 (B. Pascal) 与他合作来写这样一本书 (*Fe.*II,299–300); 当然他知道帕斯卡写文章的才能远在他自己之上. 帕斯卡表现得对此没有兴趣并委婉地拒绝了这个提议 (*Fe.*II,314); 他的观点可能更像惠更斯的. 在费马 1665 年逝世后, 有许多人要求发表他的著述, 而这些几乎没有任何一篇曾付印过. 1670 年, 他的儿子塞缪尔 (Samuel)出版了巴歇的《丢番图》重印本, 其中包括费马的边白注记以及一篇由耶稣会教士雅克 · 德 · 比利 (Jacques de Billy) 写的、关于解某类称作丢番图方程的费马方法的短文. 在此之后的 1679 年, 仍由塞缪尔出版了一卷他父亲的《*Varia Opera*》, 包括了几封有算术内容的信件. 但是对此, 接下来的半个世纪中它没有产生任何影响: 在此期间, 数论似乎死过去了.

至于它复活的日子我们则可指得一清二楚. 在 1729 年, 年轻的欧拉是圣彼得堡新成立的科学院的助理院士; 他的朋友也是他的资助人的哥德巴赫 (Goldbach) 当时在莫斯科. 他们之间的通信信件被小心地保存了起来, 并由欧拉的曾外孙于1843 年将其出版. 哥德巴赫以他自己的业余方式对数学怀着强烈的兴趣, 特别是对 "数"; 就是在给欧拉的一封信中他提出了至今还冠以他姓名的猜想. 在 1729 年 12 月的第一天, 哥德巴赫询问欧拉对于费马的下述陈述的看法, 即所有整数 $2^{2^n}+1$ 都是素数 (参考下文的第三章 §4). 在回答中, 欧拉表达了一些怀疑; 在 7 月 4 日之前没有出现任何新的说法, 然而到了这一天, 欧拉宣称他 "只不过一直在研读费马", 并对费马断言每个整数都是四个平方数的和 (也是三个三角数、五个五角数的和, 等等) 印象深刻. 从这一天起, 欧拉再也没有忘记过这个课题以及——从大的方面说——数论学科; 终于拉格朗日跟着做了, 然后是勒让德, 再后是高斯, 数论也随着他达到了完全成熟的境地. 尽管它从来不是一个通俗的学科, 但从那时以来它却一直做得十分出色.

因此对于费马以后的数论, 对于学科内部的协调, 以及它的发展的连贯性都可以做到完全公正的叙述. 相反地, 仅就费马当初不得不从一个三世纪的希腊

*4 1629—1695, 杰出的荷兰数学家、天文学家、物理学家以及钟表专家.

*5 1616—1703, 英国数学家, 剑桥大学教授, 有多种著述, 包括著名的《无穷算术》.

*6 1623—1662, 著名的数学家、物理学家兼神学家, 在几何、概率论等方面有很大的贡献, 还发明了计算机器, 在物理上有著名的帕斯卡定律.

作者那里获取灵感这个广为人知的事实来说, 它不但显示了早期数学研究的特性, 而且也指出了在过去的时代中, 重要的知识来源一直在频繁地消失和再现. 想要成为古代数学 (不管是希腊的还是美索不达米亚的) 和中世纪数学 (西方的或东方的) 史学家的人, 只涉及描述相对比较少数的几个从不为人知的海洋中偶然冒出来的岛屿是绝对有必要的, 同时也只能限于叙述那些不足信的、猜测式的东西, 譬如对沉没了的各大陆进行再造, 猜测这些大陆必定曾有过飞架其间的大桥之类. 连贯性对于历史似乎是至关重要的, 缺少了它, 他的著述最好能改叫其他的名字: 它不是史前史 (prehistory), 因为它要依靠文字的来源; 似乎叫做原史 (protohistory)*[7]更为贴切.

当然, 新的文本还会冒出来; 的确, 随时会发生. 我们关于阿基米德 (Archimedes)的知识, 因 1906 年在伊斯坦布尔发现的重写本而大大丰富了. 丢番图存世的一共由六章或叫六 "书" 组成, 而在序言中却宣称有十三书; 最近在一份阿拉伯文的手稿中发现了某些重写过的、或者也许是从原文翻译的属于丢番图的新资料; 更多的这类东西仍会出现. 重要的楔形文文本可能仍然被埋在美索不达米亚的地下, 甚至更可能 (根据诺伊格鲍尔 (Neugebauer) *[8]所言) 就在我们图书馆的盖满尘土的地下室里. 以刻痕表示的阿拉伯文和拉丁文的中世纪手稿还有待识别, 即便已清理好了的图书馆也在此列. 那么, 我们一直想要得到一幅早期希腊数学的完美图画的愿望还能实现吗? 在公元前三世纪, 欧德莫斯*[9] (Eudemos,他自己不是个数学家) 写了有四 "书" 的几何史, 它的一些片段已保留下来. 但是他那至少包含两书的算术史的内容可能已全部而且永远地丢失了吗? 即使它有部分涉及我们可将其看为代数的课题, 那么其中有一些必定是数论. 试图从哲学家们的著作中, 甚至从那些公开宣称高度尊重数学的人给出的线索和暗示来重新构建这样的发展过程大体上是徒劳的, 就如同由洛克 (Locke) 和伏尔泰 (Voltaire) *[10]的著作中要重造牛顿的《*Principia*》、从伯克利 (Berkeley) 大主教*[11] 的批判文中重建微分学是一样的徒劳.

根据十七世纪以前的数论学家的少量遗迹, 对几处精彩场面进行简短叙述便是我们的目的, 我们无意宣称做到了完美无缺. 我也尽力排除了那些属于更像是真正代数的材料 (譬如, 线性方程组和线性系的解), 但是这两个学科间的区分远非一清二楚.

---

*[7]在国内对此词的翻译和界定颇有争议, 姑择其一.

*[8]O. 诺伊格鲍尔 (1899—1990) 是杰出的古代数学史家和数学索引编纂家, 创办了《数学摘要》和《数学评论》.

*[9]哲学家. 他也是第一位科学史学家, 在亚里士多德的帮助下著了希腊史、数学和天文学史.

*[10]分别为英国和法国的哲学家, 后者非常赞赏牛顿的发现.

*[11]曾写书批判牛顿的微分学.

§1.2 素数和因数分解

在古代数学的所有课题之中, 最清楚不过属于数论的或许应该是关于正整数的基本乘法性质的那个; 它们在欧几里得的 "书" VII,VIII 和 IX 中得到了尽善尽美的处理. 一般都认为, 这些书的内容即便不是全部, 也是大量源自更早的年代, 但几乎无人能说出它们背后的故事. 关于可除性的一些事实在美索不达米亚*12必定就已经知道了; 在 60 进制中的任一块倒数表都清晰指出了那些只含有素数 2, 3 和 5 的整数和所有其他整数的区别. 埃及数学中分式加法的严格处理最终以整数比的乘法处理形式补充到了希腊的数学中, 这表明了一种基本态度的转变, 按照保尔 · 塔纳里*13 (Paul Tannery) 的非常貌似真实的假说, 有充分的理由表明它的根源在音乐理论之中. 转过来说, 这可能与最简单的平方根诸如 $\sqrt{2}$ 和 $\sqrt{5}$ 的无理性的早期证明有一些关系, 但我们并不知道那些证明是什么; 亚里士多德在一次讨论有关证明的逻辑结构 (*Analytica Priora* I.23) 的过程中如果真的暗示了对 $\sqrt{2}$ 的证明, 那么我们就没有理由把它归功于假设性的 "毕达哥拉斯学派" 了. 素数, 连同因子, 以及对给定的一些整数的公倍数的概念, 可能相当早就有之; 我们所能讲的全部是, 柏拉图 (Plato) 在他后期的著作《法律 (*The Laws*)》(737e–738a) 中提到数 5040 的一些性质, 着重指出它是直到 10 的那些数的公倍数 (但 2520 也是), 并且如果不算 5040 自己, 它有 59 个因子; 这表明在柏拉图的科学院里的数学家们对于整数的分解已经具有了一些先进的知识, 但不能确定有多少. 是否在 *Eucl.*VII,1–2 中求两个整数的最大公因子 (g.c.d.) 的所谓 "欧几里得辗转相除法" 与应用于可能无公度的量的这个同一方法的理论 (*Eucl.*X,2) 之间原本就有一种联系? 一个数学方法在不同的场合被发现了两次, 并且过了长时间才认识到这两个发现本质上是相同的, 这不是常常发生的吗? 数学上一些重要进展也正是以这种方式出现的.

甚至在欧几里得那里, 我们也找不到对于将整数分解为素数因子的唯一性的一般证明; 的确, 或许他已注意到此, 然而他全部所做的不过是关于对任意多个给定素数的最小公倍数 (l.c.m.) 的一个陈述 (*Eucl.*IX,14) 罢了. 最后, 对于存在无限多个素数的证明 (*Eucl.*IX,20) 无疑代表了一个重大进展, 但是并没有令人信服的理由表明应将此归于欧几里得或者追溯到更早的年代. 与我们目的相关的是在以后的诸多世纪里欧几里得的极其广泛的传播, 虽然所有原先的内容都已被清除, 但从那时以来, 它成为了数学家普遍可用的知识宝库.

---

*12作者这里指的是古巴比伦, 大约是公元前三十世纪到公元前 729 年的时期.

*131843—1904, 法国数学家与数学史学家, 曾参与笛卡儿 (Descartes)全集的翻译.

§1.3 完全数

在许多世纪中都发现了数的不可思议的或神秘的性质. 不知何故, 不管是在古希腊还是更早, 已将完全性的概念赋予了那些等于它们自己的因子和的整数. 在欧几里得算术书最后的一个定理中 (*Eucl.*IX,36), 照它们的作者的观点看或许这是他的数论工作的顶点吧, 它断言 $2^n(2^{n+1}-1)$ 当第二个因子为素数时是个完全数 (perfect numbers). 这个课题连同它的一些推广 (诸如一对 "亲和" 的数)还零零星星地出现在后来的工作中, 这大概是因为赋予这个概念的名称的特殊吸引力的缘故吧. 它其实并不具有理论上的重要性, 如果不是因为它吸引了一大批费马的同时代人, 像梅森*14 (M. Mersenne) 和弗莱尼柯*15 (B. Frenicle), 甚至它在费马自己的初期的研究 (参看下文的第二章 §4) 中也起了一些作用, 我们也不会提到它.

§1.4 一次问题

在整数中求一次不定方程的解必定早就在许多世纪中, 或是作为谜语 (在希腊《文选 (*Anthology*)》的各种小警句便是好的例证 (参看 *Dioph.*,vol.II,pp. 43–72)), 或是作为历法问题就出现了; 当然, 数学家对后者更感兴趣. 这类的一个典型问题可以用一个双重同余式

$$x \equiv p \pmod a, \quad x \equiv q \pmod b$$

来表述, 或者作为线性同余式 $ax \equiv m \pmod b$, 也或者作为一个整数方程 $ax - by = m$ 来表述. 对其求解的一般方法, 本质上等同于求 a 和 b 的 g.c.d. 的 "欧几里得辗转相除法" (*Eucl.*VII,2) 或者 (用现代的术语) 也等同于对连分式 (continued fraction) a/b 的计算; 这两个问题真的如此相近, 以致谁要是知道如何解这一个, 如果有必要的话, 则解另一个便几乎不会失败. 但是, 如果不谈中国的话, 对一般解的第一个明确叙述出现在五到六世纪的梵语天文著作《*Āryabhaṭīya*》中 (参看譬如 Datta和 Singh 所著《印度数学史 (*History of Hindu Mathematics*)》, Lahore,1938,vol.II,pp.93–99). 在后来的梵文文本中这被称作 *kuṭṭaka* (="粉粹机") 方法; 如果想起费马的 "无限下降法", 这确实是一个相称的名字. 因为那个时期的印度天文学大体上基于源自希腊的知识, 有人非常想将这同一个来源也归因于 *kuṭṭaka*, 但自然也缺少证明.

*14 1588—1648, 数学家, 教士; 主要研究领域为数论; 因以作为杰出哲学家和科学家的信件媒介人而知名. 后文将多次提及他.

*15 1612?—1675, 法国数学家, 主要研究领域为数论和组合学.

然后, 在 1621 年, 巴歇颇为幸运地没留意到 (自然地) 他的印度先行者, 也没有留意到与欧几里得的 "书" VII 的关联, 在他的对 *Dioph.*IV,41_b (= IV, 36 的引理) 的评论中强力地公示了与此一样的方法, 并宣布要在一本算术 "原理" 的书中发表它; 因为这个书从未面世过, 他便把它塞进了他的《令人愉悦和舒心的问题 (*Problèmes plaisants et délectales*)》的第二版 (里昂, 1624) 中, 费马和沃利斯发现了它的藏身之处; 的确, 他们两个太熟知他们的欧几里得了, 不会不认识这里的欧几里得辗转相除法.

§1.5　毕达哥拉斯三角形

对于算术级数 (诸如 $\sum_1^N n$)、几何级数 (诸如 $\sum_0^N 2^n$) 以及高阶算术级数 (诸如 $\sum_1^N n^2$) 的求和, 无需在此列举许多来源, 不管是美索不达米亚的还是希腊的; 只要涉及希腊, 这就不可能将其与 "垛积数 (figurative numbers)" 分开. 最原始的一类列表法可直接导出了不少这类公式 (譬如 n^2 = 前 n 个奇数和), 因而也可用适当的图表来验证. 这样的结果必定较早就已广为人知；诉求于毕达哥拉斯名字的光环于我们对事情的了解少有裨益.

关于 "毕达哥拉斯" 三角形也可说出同样一番话来, 对此术语我们只理解为一些整数的三元组 (a, b, c), 它们满足

$$(1)\qquad a^2 + b^2 = c^2,$$

因此, 假如我们还记得有个冠以毕达哥拉斯的名字的几何定理的话, 那就测量一下一个直角三角形的各个边长吧. 当然, 如果 (a, b, c) 是这种数, 那么 (b, a, c) 也如此; 在容许这个置换时, (1) 的通解由

$$(2)\qquad a = d \times 2pq, \quad b = d \times (p^2 - q^2), \quad c = d \times (p^2 + q^2)$$

给出, 其中 p, q 互素, $p - q$ 为奇数且 > 0; 于是 d 是 a, b, c 的 g.c.d. 取 $d = 1$, 得到 (差一个在其上的置换而唯一决定) 了 (1) 互素整数组的通解. 最简单的这样的三元组自然是 $(3, 4, 5)$, 似乎从非常早的年代起它就属于某种数学的民间传说了.

在古巴比伦的泥板 PLIMPTON 322 上保存了十五个这种毕达哥拉斯三元组的表格, 由 O. 诺伊格鲍尔和 A. 萨赫斯 (Sachs) 发表 (《数学的楔形文文本 (*Mathematical Cuneiform Text*)》, New Haven 1945, pp.38–41), 他们所测定的年代为公元前 1900 年与 1600 年之间. 或许它们是借助于三角几何计算出来的; 但它必定根据了某些公式, 或者就是 (2), 或者更简单地是关系式

$$a^2 = (c + b)(c - b);$$

a 的值都取作 "正则" 数 (除 2, 3, 5 外不含其他的素因子), 而 a^2/b^2 的值从 1 几乎到 $\frac{1}{3}$, 以确定的间隔按递降的次序排列.

唉, 一切都太过轻松地归结到与 "毕达哥拉斯" 相似的知识了; 若用普洛克拉斯 (Proclus)*[16]的话说, 这只不过是转移和回避问题罢了. 好吧, 其实容易做出断言: 要么他们重新发现了它, 要么 (更可能一些) 它通过还不为人知的渠道从美索不达米亚传给了他们. 可以确定的是, 欧几里得已知道了上述构造毕达哥拉斯三元组的公式, 他在 *Eucl.*X,29 的引理中证明了它们; 五个世纪之后, 丢番图是如此地熟悉它们, 以致他有一个专业词 (πλάσσειν "塑造") 表示从一对整数 (p,q) 来决定三角形 $(2pq, p^2-q^2, p^2+q^2)$ 的构造. 无论那个课题在中世纪的命运是什么, 它却又一次披上了丢番图的外衣出现在邦贝利*[17] (Bombelli) 1572 年的《代数学 (*Algebra*)》之中, 它的 "书" III 几乎完全基于邦贝利对梵蒂冈图书馆中丢番图的一份手稿的仔细研读上. 然后, 这个课题又被韦达*[18] 捡起, 最初出现在他的《*Notae priores*》(在 1631 年出版前其复印本已流传很久), 而后则在他 1593 年的《*Zetetica*》中; 两者大体上都来自丢番图, 韦达可能从克西兰德 (Xylander)1575 年的拉丁译本读到它, 但更有可能是在巴黎的皇家图书馆研究过它的一份希腊文手稿. 韦达的著作在处理丢番图资料时比邦贝利展示了更多的原创性, 我们将在以后要更仔细地讨论它.

§1.6 两个平方数的和

不管人们是对毕达哥拉斯三角形还是对两个平方数的和感兴趣, 都不可避免地总要碰到一个关键之处, 在那里, 代数恒等式

$$(3)\qquad (x^2+y^2)(z^2+t^2)=(xz\pm yt)^2+(xt\mp yz)^2$$

必定要起作用. 特别地, 由于右端的双重符号, 只要人们希望有多于一个的方式将一个数表示为两个平方数的和时, 它就会出现. 对于 $z=t=1$, 得到了特殊情形

$$(4)\qquad 2(x^2+y^2)=(x+y)^2+(x-y)^2,$$

它穿上几何的外衣出现在 *Eucl.*II,9–10 中.

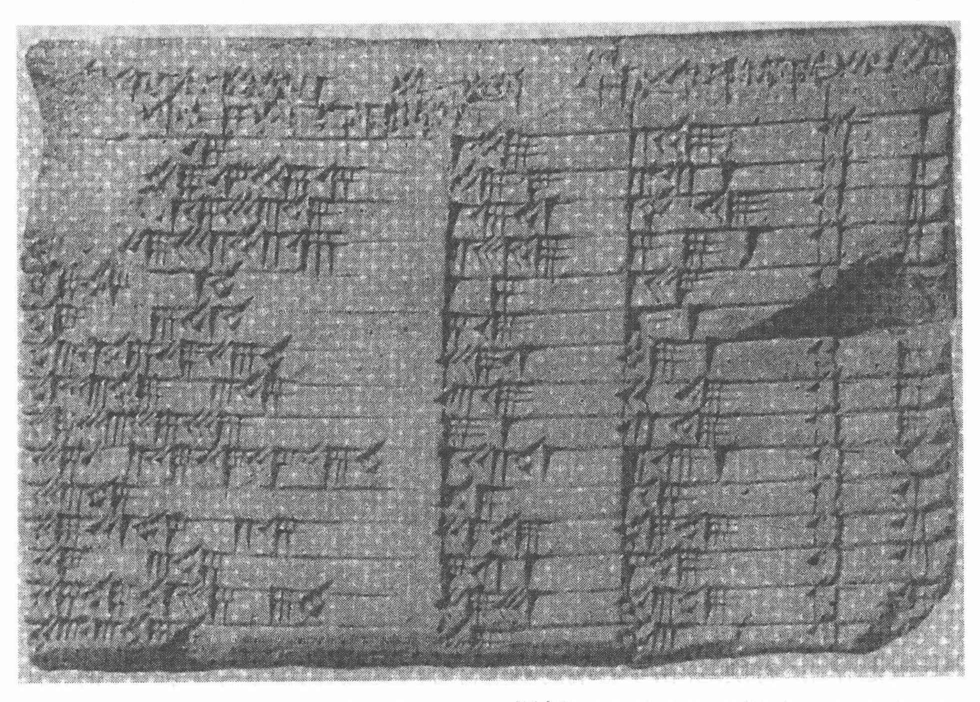
恒等式 (3) 一定为丢番图所熟知, 这可表现在下面的段落 (*Dioph.*III.19) 中:

"65 有如下一个性质: 它可以以两种不同的方式表示为两个平方数的和, 即

*[16]412—485, 希腊数学家及哲学家, 著有对欧几里得《原本》的评述等.

*[17]1526—1572, 意大利数学家, 公认是西方第一个定义了负数的人.

*[18]1540—1603, 法国数学家, 在解方程和几何有诸多贡献; 著名的韦达定理即归于他. 见本章 §12.



PLIMOTON (泥板) 322

为 16+49 和 64+1; 之所以如此, 是由于它是 13 和 5 的乘积, 而它们的每一个都是两个平方和."

由于丢番图对一本现已失散了的书《辅助定理 (*Porisms*)》有多处的参考, 并且由于 (3) 在 $y=t=1, x-z=\pm 1$ 的特殊情形, 即恒等式

$$(x^2+1)(z^2+1)=(xz+1)^2+1,$$

或者进一步等价地,

$$x^2z^2+x^2+z^2=(xz+1)^2,$$

在 $x-z=\pm 1$ 的情形也似乎隐含在某个这样的参考材料之中 (*Dioph.*V,5;参看 *Dioph.*III,15), 或许想象 (3) 可能就是他的《辅助定理》之一也不算太牵强附会吧. 当巴歇将 (3) 作为他的《辅助定理》的命题 III.7 包含在他的《丢番图》中时, 这必定也是他的观点. 但是, 尽管有点不太合理, 其实前面所引述段落也有可以用来否认 (3) 的知识属于丢番图; 但之前我们根本不知道在哪里有对 (3) 的明晰陈述, 直到我们找到了在 1225 年才出版的斐波那契*19 (Fibonacci) 的《平方数 (*Liber Quadratorum*)》(*Leon.*II,257–260=*LVE.* 命题 IV). 但斐波那契宣称他并不信任它, 似乎宁愿只把它当作一个为专家熟知又值得广泛传播的结果.

与斐波那契的更受欢迎的《算盘 (*Liber Abaci*)》相反, 他的《平方数》则落得被人深深遗忘的境地; 几经艰难, 它的一个复印本才被邦孔帕尼*20 (Prince Boncompagni) 找到, 并在 1856 年将其出版. 在前面已说过, 邦贝利在他 1572 年的《代数》中用了许多从丢番图抄来问题; 特别地, 他的 "书" III 的问题 CXXVI 就是从 *Dioph.*III,19 直接翻译过去的, 另外还包括了我们在前面所引述的关于 65 可以以两种方式表示为两个平方和的段落; 但是他没说是否理解了它所涉及的内容. 决定性的步骤是由韦达采取的, 他将 (3) 用到从两个已知的直角三角形来构造两个新的直角三角形上, 根据所使用 (3) 中的符号, 他分别称这个运作为 "*synaeresis*" 或者 "*diaeresis*" (参看《*Notae priores*》, 命题 XLVI=*Op.* p.34; *Zet.*IV,2=*Op.*pp.62–63). 韦达远不是只把自己局限在毕达哥拉斯三元组和整数的人, 但偶然间, 他满意地注意到他的构造和恒等式对于任意的量都成立. 他也成功地指出了 (《*Notae priores*》, 命题 XLVIII) 在 (3) 和三角函数的加法与乘法之间的关系; 只要我们令

$$x=r\cos\alpha,\quad y=r\sin\alpha,\quad z=s\cos\beta,\quad t=s\sin\beta,$$

从而

$$xz\pm yt=rs\cos(\alpha\mp\beta),\quad xt\mp yz=rs\sin(\alpha\mp\beta),$$

*19 1170?—1240?, 意大利数学家, 有多种著述. 参看 §1.7.

*20 1821—1894, 出身于意大利显赫的贵族世家, 创办了《数理科学史与文献通报》.

我们便能清晰看出这个关系; 另外, 他还对 $(x, y) = (z, t)$ 的情形引进了术语 "双角 (angle-duplication)". 就像上面表明的那样, 韦达对于代数和几何的兴趣要比对数论的大得多 (也可参考他的《*Theoremata ad Angul. Sect.*》$=$ *Op.*pp.287–304).

§1.7 斐波那契和《平方数》

在这里, 对于斐波那契和他的《平方数 (*Liber Quadratorum*)》多说几句话应该还不算是出格. 斐波那契, 也被叫做列昂拉多 · 皮萨诺 (Leonardo Pisano), 他是一个喜爱旅行、博闻、无疑也是博学的数学家. 他出生在作为一个国际商会成员的家庭, 住在从东到西的地中海沿岸地区, 出生地为比萨, 推测起来大概在 1170 年左右. 他曾生活在北非和君士坦丁堡, 并且在十二世纪后期至少访问过西西里、普罗旺斯、叙利亚和埃及, 他走到哪里就从当时最有学问的数学家那里收集信息, 这些多发生在他作为令人羡慕的数学专家和教师的职位安定在故乡下来之前. 当腓特烈二世 (Frederic II) 皇帝逗留在那里时, 列昂拉多当然被召见, 并被介绍给了朝廷的圈子, 在当时这是一个拉丁、阿拉伯和希腊文化的交汇场合; 难以想象, 列昂拉多竟对所有这三种语言都有一定程度的熟悉. 这是那个时代的时尚, 因此他在腓特烈面前得到了皇家随从的最有学问的人的声誉. 在某个场合, 他被挑战要求找出 3 个平方数, 他们组成公差为 5 的算术级数, 即以现代的公式表达便是在有理数中解

$$y^2 - x^2 = z^2 - y^2 = 5,$$

或者等同于在整数中解

$$Y^2 - X^2 = Z^2 - Y^2 = 5T^2.$$

这成了《平方数》的讨论对象.

关于组成算术级数的平方数问题是十分古老的; 由于恒等式 (4), 也就是 *Eucl.*II,9–10, 找出这样的平方数等价于找出毕达哥拉斯三角形. 事实上, 如果 X^2, Y^2, Z^2 成为算术级数, 我们则有

$$Y^2 = \frac{1}{2}(X^2 + Z^2) = U^2 + V^2,$$

其中 $U = \frac{1}{2}(X+Z)$, $V = \frac{1}{2}(Z-X)$, 而差 $Y^2 - X^2 = Z^2 - Y^2$ 的值为 $\frac{1}{2}(Z^2 - X^2) = 2UV$, 它等于三角形 (U, V, Y) 的面积的四倍. 没有任何证据告诉我们列昂拉多的挑战者或者列昂拉多自己已知道了这个事实. 但是难道它与下面的事实仅仅是偶然一致的吗? 这个事实是, 现在在伊斯坦布尔的老皇宫图书馆保存了一份十一或者十二世纪的拜占庭手稿, 其中有这样的问题: " 求一个面积为 $5m^2$ 的

毕达哥拉斯三角形". 这份手稿已由 Heiberg出版 (*Bibl. Math.*(III) 8 (1907–08), p.122); 列昂拉多可能在君士坦丁堡看到过它. 该问题的作者知道一个毕达哥拉斯三角形的面积是 6 的一个倍数; 他说, "因此, 我们取 m^2 为 6 的倍数"; 取 $m = 6$, 没有做任何解释他就写下了这个三角形 $(9, 40, 41)$, 面积为 $180 = 5 \times 6^2$. 成算术级数的平方数为 $31^2, 41^2, 49^2$, 它已同样地出现在 *Dioph.*III,7 中.

另一方面, 列昂拉多对他的问题应用了一个吸引人的、显然是原创的方法, 它基于系统地将每个整的平方数 n^2 当作前 n 个奇数之和, 它的每一步都可以用适当的图来解释. 他的第一个重要结果 (*Leon.* II.265–271=*LVE.* 命题 XI–XII) 等于说 $Y^2 - X^2 = Z^2 - Y^2 = D$ 具有整数解 X, Y, Z 当且仅当 D 具有形式

$$D = 4d^2pq(p^2 - q^2) = 4d^2pq(p+q)(p-q),$$

其中 d, p, q 同于前面 (2) 中的; 当然这个 D 是 4 倍于 (2) 中给出的面积. 然后他指出 D 必是 24 的倍数, 从而最后他解决了他的问题: 令 $d = 1, p = 5, q = 4$, 对应 $D = 5 \times 12^2$ 以及与前面相同的平方数 $31^2, 41^2, 49^2$. 最后, 他观察到, 除 5 以外还有其他整数具有同样的性质 (譬如 7, 取 $p = 16, q = 9$ 则出现一样的情形), 但是许多数不是这样的; 他还断言 D 绝不会是一个平方数, 但给出的理由是完全不恰当的; 这个断言的确为真, 不过却是费马的重要发现之一 (参看第二章 §10).

§1.8 关于佩尔 (Pell) 方程的早期工作

正如恒等式 (3) 在对两个平方数和的任何讨论中起着重要作用一样, 恒等式

$$(5) \qquad (x^2 - Ny^2)(z^2 - Nt^2) = (xz \pm Nyt)^2 - N(xt \pm yz)^2,$$

$$(6) \qquad (x^2 + Ny^2)(z^2 + Nt^2) = (xz \pm Nyt)^2 + N(xt \mp yz)^2,$$

其中 N 是一个正整数, 在依赖于二次型 $X^2 \mp NY^2$ 的那些问题中也起着相似的作用. 当然, 从现代代数的观点看, 他们与 (3) 没有真正的差异, 但是直到十八世纪前还没有完全意识到这点. 就我们而言, 或许验证 (5) 和 (6) 的最简单方法是写下

$$(x + y\sqrt{N})(z \pm t\sqrt{N}) = (xz \pm Nyt) \pm (xt \pm yz)\sqrt{N},$$

以及同一恒等式但在其中以 $\sqrt{-N}$ 代替 $\sqrt{N}$, 然后两端乘以由将 $-\sqrt{\pm N}$ 替换 $\sqrt{\pm N}$ 得到的共轭量; 这是欧拉首先在他 1770 年的《代数》(*Eu.*I-1,422,Art.175) 中指出的. 由于欧几里得将他的整个 "书" X 全都用来讨论二次无理性理论上

了, 人们不禁想象他, 或者他的一个后继者, 可能已经考虑过 (5), 或至少 (5) 的特殊情形的某种推导. 不仅欧几里得他自己充分注意到关系式

$$(\sqrt{r}+\sqrt{s})(\sqrt{r}-\sqrt{s})=r-s,$$

并且, 甚至恒等式

$$\frac{1}{\sqrt{r}+\sqrt{s}}=\frac{\sqrt{r}}{r-s}-\frac{\sqrt{s}}{r-s} \tag{7}$$

都可以看作是那本书中命题 112 的实质内容. 可惜, 欧几里得在 "书" X 中的动机似乎是希望对于正多边形和正多面体理论建造一个普遍的架构, 而不是像现代数学家那样把它当作了一个二次域的代数理论. 于是把它留给我们来凭空推测, 是否在远古或稍后的年代里, 那种含有平方根的恒等式在算术著述中可能从来就没有使用过, 至少是探索性的那种使用. 的确如此, 迟至十八世纪, 欧拉和拉格朗日还觉得为把虚平方根引进数论这个原创思想而相互祝贺是挺合时宜的 (参看下文的第三章 §14).

有人颇有根据地认为 $x^2-Ny^2=\pm m$, 其中 N, m 为正整数这种类型的方程必定很早就在希腊出现过, 它可能与在 N 不是平方数时为得到 $\sqrt{N}$ 好的有理近似值有关. 可以清楚看出, 如果 $x^2-Ny^2=\pm m$, 并且如果 x 和 y 比起 m 更大的话, 那么 x 与 y 的比值便给出了 $\sqrt{N}$ 一个好的近似值, 这是因为它清晰地显示在恒等式

$$\frac{x}{y}-\sqrt{N}=\frac{1}{y}\frac{x^2-Ny^2}{x+y\sqrt{N}}$$

之中, 而这是 (7), 即 *Eucl.*X,112 的一个特殊情形. 因此当欧托基奥斯*[21]在他关于阿基米德的评论 (*Arch.*III,234 与 246) 中, 想要验证阿基米德对于 $\sqrt{3}$ 的近似值 265 : 153 和 1351 : 780 的有效性, 他只是写下了

$$265^2-3\times153^2=-2,\quad 1351^2-3\times780^2=1.$$

现在, 一旦你知道了其中的一个解以及 $p^2-Nq^2=\pm1$ 或者 $=\pm2$ 的一个解, (5) 便给出了构造 $x^2-Ny^2=\pm m$ 这种解的简便方法 (参考下文的 §9). 譬如, 阿基米德对 $\sqrt{3}$ 的近似值最好解释为他系统地应用了公式

$$(5x+9y)^2-3\times(3x+5y)^2=-2\times(x^2-3y^2),$$

也就是 (5) 的特殊情形 $N=3, z=5, t=3$ (参考 W.Knorr, *Arch.f.Hist.of Ex.Sc.* 15(1975),pp.137–138). 在这里, 应该注意: 如果 $x^2-3y^2=-2$, 那么 x 和 y 必定

*[21]Eutocius of Ascalon, 480?—?, 写过三本对于阿基米德著作, 包括《论球和圆柱》的评论.

都是奇数, 而 $5x+9y$ 和 $3x+5y$ 则都是偶数; 上述关系式便成为

$$\left(\frac{5x+9y}{2}\right)^2-3\left(\frac{3x+5y}{2}\right)^2=-\frac{1}{2}(x^2-3y^2).$$

事实上, 阿基米德对于 $\sqrt{3}$ 的近似值全都以 $5^2-3\times 3^2=-2$ 开始并交替地应用变换

$$(x,y)\mapsto\left(\frac{5x+9y}{2},\frac{3x+5y}{2}\right)$$

和

$$(x,y)\mapsto(5x+9y,3x+5y).$$

这同一个方法的例子可能在更早的时期就有, 但首先由塞翁*22 (Theon of Smyrna) 在公元二世纪用所谓 "边和对角线数" 给出的例子所证实, 这就是从 $x^2-2y^2=\pm 1$ 的明显的解 $x=y=1$ 出发, 用变换

$$(x,y)\mapsto(x+2y,x+y)$$

进行迭代得出 $x^2-2y^2=\pm 1$ 的逐次解. 这个过程的有效性在于恒等式

$$(x+2y)^2-2\times(x+y)^2=-(x^2-2y^2);$$

这是 (5) 的特殊情形 $N=2, z=t=1$, 但也等价于 (4), 即 *Eucl.*II,9–10. 赋予这个方法的名字强调指出了它与正方形的对角线和边的比 $\sqrt{2}$ 的关系.

我们又再一次在丢番图那里发现了至少是上述恒等式的踪迹, 其中 (5) 和 (6) 的情形 $y=1, t=1$ 或 2, $xt-z=\pm 1$ 似乎隐含在 *Dioph.*V,3 和 *Dioph.*V,4 中; 前面的段落中有一个对《辅助定理》明晰的参考, 这又让我们推测那些《辅助定理》可能包含了许多这样的恒等式, 或许甚至 (5), (6) 也在其中; 它们包含了十分精巧代数等式这一点从 *Dioph.*V,5 和 V,16 的参考文献便已清楚显现. 尽管这必定只是一个猜想, 但我们确实还是发现了对 (5) 的一个明晰的陈述, 它出现在一个叫做婆罗摩笈多*23 (Brahmagupta) 的七世纪的天文学家和数学家的著作中; 当然是与形如 $x^2-Ny^2=\pm m$ 问题有关的 (*Col.*,363; 参考 Datta 和 Singh, 同上, vol.11,pp.146–148). 在这里还可提出关于 (5) 的希腊来源的问题, 但也回答不了.

---

*22希腊科学家, 编有包含算术、几何、天文、音乐等方面的手册.

*23598—665?, 他在《婆罗摩修正体系》中给出了正负数的四则运算法则.

§1.9　佩尔方程: 阿基米德和印度人

1773 年, 德国的一个文学界人物、著名的沃尔芬比特 (Wolfenbüttel) 图书馆馆员莱辛*24 (Lessing) 发表了一首希腊文的 "epigram(警句)", 即一首短诗 (22 个对句), 它出现在他掌管的手稿里新近发现的一份中. 这份手稿说它是阿基米德作为问题交给在亚历山大城的数学家们的.

已经有不少的数学 epigrams 为众人所知. 其中大多数说的都是浅显的问题, 而莱辛发现的不在此列; 的确有一切理由支持它应归属于阿基米德, 也没有人提出过怀疑. 只是对它如何诠释的问题一定还没有得到解决.

我们要在此 (*Arch.*II,528–534) 处理一个具 8 个未知整数的问题; 我们以 x,y,z,t,x',y',z',t' 表示它们. 第一个 8 个对句以完全标准的形式叙述了三个方程的一个组:

$$x-\left(\frac{1}{2}+\frac{1}{3}\right)y=y-\left(\frac{1}{4}+\frac{1}{5}\right)z=z-\left(\frac{1}{6}+\frac{1}{7}\right)x=t;$$

当然, 这表明了他对于线性方程组具有相当高的熟悉程度, 而在其他方面则说不出什么. 准确到一个因子的解为

$$x_0=2226,\quad y_0=1602,\quad z_0=1580,\quad t_0=891.$$

在接着的 5 个对句中我们有了下面的四个方程:

$$x'=\left(\frac{1}{3}+\frac{1}{4}\right)(y+y'),\quad y'=\left(\frac{1}{4}+\frac{1}{5}\right)(z+z'),$$
$$z'=\left(\frac{1}{5}+\frac{1}{6}\right)(t+t'),\quad t'=\left(\frac{1}{6}+\frac{1}{7}\right)(x+x').$$

在这里事情显得有一点复杂, 但该 epigram 的注释者或者它的提供者 (自然没有注明时间) 已经能够得到了一个解. 由于 x',y',z',t' 必须是整数, 结论便是, 我们必定有

$$(x,y,z,t)=n\times 4657\times(x_0,y_0,z_0,t_0),$$

其中 n 为整数; 而 x',y',z',t' 则可相应地算出来. 在注释者给出的数值解中我们有 (当然未必一定是)$n=80$.

至此所做的只是线性代数; 作者说:" 如果你能把问题解到这里, 便没有人敢说你无知, 但这并不表明你已是个专家; 来吧, 告诉我后面的事情"; 于是他在两个对句中说道, $x+y$ 必须是个平方数, 又在另两个对句中说, $z+t$ 必须是三角

*24 1729—1781, 是位有影响的德国文艺理论家、剧作家. 作品有《拉奥孔, 或论画与诗的界限》、《汉堡剧评》、《萨拉 · 萨姆逊小姐》等.

数; 最后他说:"如果你做出来了, 你便赢得了最高智慧奖". 他有充分理由作如是之说: 可以证明其最小解具有 10^{103275} 的量级.

事实上, 借助于整数 n, 我们可以记 $x+y=4An$, 其中 A 不含平方因子, 故而必定有 $n=AU^2$, 而 U 为整数. 另一方面, 如果 $z+t$ 是一个三角数, 即具有形式 $\frac{1}{2}m(m+1)$, 则 $8(z+t)+1$ 必为一个平方数 V^2; 因为我们可以令 $z+t=Bn$, 故得到了 $V^2-NU^2=1$, 其中 $N=8AB$. 于是该问题等于是 "佩尔方程" 的一个特殊情形.

我们该如何理解此事呢? 从最少的方面说, 它必定表明阿基米德对这样的方程有兴趣; 或许他还对这个解集合的结构有一些洞察; 反过来这也会预示出 (5) 的信息. 从最好的方面说, 他可能已设计了对 $x^2-Ny^2=1$ 这种类型方程的一般求解方法; 不管是不是显式的, 这可能取决于 $\sqrt{N}$ 的连分式的构造, 即取决于将欧几里得辗转相除法应用于这样的平方根. 塔纳里似乎偏爱后一种说法, 并怀着这个解会在某天与消失了的丢番图的书一起重现的希望; 迄今对此尚无即将来临的显著证据. $x^2-Ny^2=1$ 类型的方程确实在丢番图那里出现过 (譬如在 *Dioph.*V,9 和 11), 但它要求的是有理解, 即使偶然地也得到了整数的解 (譬如在 *Dioph.*V,9, 那里的 N 具有 m^2+1 的形式, 给出了 $y=2m, x=2m^2+1$).

对于印度人, 尽管我们在有关他们的知识方面有巨大的缺口, 但我们却又一次有确凿的证据在手; 自科尔布鲁克*[25](H.T.Colebrooke)出版了《算术的代数及求积法—取自婆罗摩笈多和婆思古罗的梵文文献 (*Algebra with Arithmetic and Mensuration, from the Sanscrit of Brahmegupta and Bháscara*)》(London 1817) 以来, 一些重要的以英文表达的内容, 在西方已为人知. 这本可追溯到七世纪的婆罗摩笈多的著作中, 我们可以找到专门讨论方程 $Ny^2+m=x^2$ 的一整节 (Chap.XVIII,§7; *Col.*pp.363–372; 参看 Datta 和 Singh, 同上, pp.146–161), 其中 N 为正整数 (默认其为非平方数), m 是个正或负的整数, 并要求求出它的整数解 (x,y); 我们应注意, 婆罗摩笈多和他的后继者们对于正负数及 0 十分熟悉, 从而他们充分地陈述了处理它们的规则. 另外, 由婆罗摩笈多与解这些方程所引进的相关的术语也为他的后继者们所接受, 少有改动; 所讨论的这些类型的问题被他们称为 *vargsprskṛti*("平方性的"); N 为 *gunaka* ("限定元") 或者 *prakṛti* ("本性元"); m 为 *kṣepa* ("加元"); y 和 x 分别为 "第一的"、"次要的" 或 "低级的" 根, 以及 "第二的"、"主要的" 或 "高级的" 根. 就是在那一节 (64–65 行) 我们找到了恒等式 (5), 它以两种合成规律的形式给出:

$$((x,y;m),(z,t;n)) \to (xz \pm Nyt, xt \pm yz; mn),$$

*[25] 1756—1837, 英国学者, 编有梵语字典及翻译了大量的古印度文献.

其中为简便起见, 我们对任意满足 $x^2-Ny^2=m$ 的整数三元组记为 $(x,y;m)$, 而"限定元" N 则一直保持不变. 在后来的文献中这些规律以 *bhāvanā* ("复合") 法则而知名; 根据符号为 $+$ 或 $-$ 称这个 *bhāvanā* 为正或负, 并根据 $(x,y)=(z,t)$ 与否称其相等或不等. 因此这些词汇准确地对应了韦达的 *synaeresis, diaeresis* 及双角 (参看 *supra*, §VI).

像婆罗摩笈多所解释的那样, *bhāvanā* 可以以各种方式用来从已知的解推导出新的解; 例如, 当已知一个解时, 与一个三元组 $(p,q;1)$ 的合成将对一个给定的"加元" m 生成一些不确定个数的解. 类似地, 当人们将一个三元组 $(x,y;m)$ 与自己的合成时便得到了一个三元组 $(X,Y;M)$, 其中 $M=m^2$, 它给出了具加元 1 的方程的一个有理解 $(X/m,Y/m)$, 当 $X/m,Y/m$ 为整数时则给出了三元组 $(X/m,Y/m;1)$. 更一般地说, 如果 $M=\mu m^2$, 并假定 $X/m,Y/m$ 为整数, 则可由任意三元组 $(X,Y;M)$ 得到一个三元组 $(X/m,Y/m;\mu)$ (Datta 和 Singh, 同上, pp.150–151).

这些注释连同 *bhāvanā* 法则已经使得婆罗摩笈多有能力去解多种情形下的佩尔方程 $x^2-Ny^2=1$ (譬如 $N=92$ 和 $N=83$), 并且当已知在 $m=-1,m=\pm2$ 或者 $m=\pm4$ 的三元组 $(p,q;m)$ 时, 给出它的解的法则, 事实上一旦将 $(p,q;m)$ 与自己合成, 该解便为

$$(p^2+Nq^2,2pq;1),\ \text{分别地},\ \left(\frac{1}{2}(p^2+Nq^2),pq;1\right);$$

类似地, 如果 $m=\pm4$ 且 p 为偶数, 则我们有解

$$\left(\frac{1}{4}(p^2+Nq^2),\frac{1}{2}pq;1\right).$$

另一方面, 如果 $m=\pm4$ 且 p 为奇数, 则不得不合成 $(p,q;m)$ 自身两次以得到一个三元组 $(P,Q;\pm1)$, 于是, 如果符号为 $-$ 则将 $(P,Q;-1)$ 与自己合成; 对于这两种情形, 婆罗摩笈多给出了显式的公式, 它是个 p,q 的多项式, 在一种情形次数为 3, 而在另一种为 6.

即便如此, 对于一般的解这还远远不够; 自科尔布鲁克以来我们已经知道在婆什伽罗*26 (Bhāskara, 十二世纪; *Col.*pp.170–184; 参看 Datta 和 Singh, 同上,pp.161–172) 的著作中可以找到这样一个解, 但是现在在一份十一世纪的注释文稿中也发现了一个几乎完全一样的表述, 它归属于一位以前不为人所知的作者伽耶德瓦 (Jayadeva) (参考 K.S. Shukla 的《*Gaṇita* 5》(1954), pp.1–20). 这两位作者都把这个方法形容为"轮转过程" (*cakravāla*, 由 *cakra* (轮子) 而来). 所以, 它的真正的来源仍不为人知.

*26 十二世纪印度的大数学家, 给出过球面面积的计算公式.

ALGEBRA,

WITH

ARITHMETIC AND MENSURATION,

FROM THE

SANSCRIT

OF

BRAHMEGUPTA AND BHASCARA.

TRANSLATED BY

HENRY THOMAS COLEBROOKE, Esq.

F.R.S., M. LINN. AND GEOL. SOC. AND R. INST. LONDON; AS. SOC. BENGAL; AC. SC. MUNICH.

LONDON:

JOHN MURRAY, ALBEMARLE STREET.

1817.

科尔布鲁克 (H. T. Colebrooke) 的《算术的代数及求积法——取自婆罗摩笈多和罢思古罗的梵文文献》的扉页

就如许多杰出的发现的情形一样, 这个发现也可以以回顾的方式看成是由更早期工作的极其自然的推导. 对于已知的 N, 假定我们有了一个三元组 $(p,q;m)$, m 是在某种意义下的一个小的数; 我们希望由此推导出另外的这类三元组. 为此, 我们构造一个三元组 $(x,y;M)$, 其中 $M=mm'$ 且 m' 是个小的数; 将其与第一个合成便得到了三元组 $(X,Y;m^2m')$; 如果现在 X 和 Y 是 m 的倍数, 这是便给了我们一个三元组 $(p',q';m')$, 其中 $p'=X/m$, $q'=Y/m$, 从而我们可以以同样的方式进行下去, 希望可最终得到一个三元组 $(u,v;1)$. 在 *cakravāla* 中这是由取 $y=1$ 从而 $M=x^2-N$ 得到的, 其中的 x 留着等待适当的选择. 这给出了

$$X=px+Nq,\quad Y=p+qx.$$

我们可假设 q 与 m 互素; 如果不是如此, 关系式 $p^2-Nq^2=m$ 就会表明 p 和 q 有一个最大公因子 $d>1$, 并且 m 就会是 d^2 的倍数, 故而三元组 $(p,q;m)$ 便可用 $(p/d,q/d;m/d^2)$ 代替了. 我们现在可用 *kuṭṭaka* (="粉粹机") 方法(参看 *supra*, §IV) 来决定 x 使得 $Y=p+qx$ 是 m 的倍数. 记

$$\begin{aligned}q^2M=q^2x^2-Nq^2&=q^2x^2-p^2+m\\&=m\times\left(\frac{qx+p}{m}\times(qx-p)+1\right),\end{aligned}$$

因为 q 与 m 互素, 我们看出 M 是 m 的倍数. 那么现在关系式 $X^2=NY^2+mM$ 表明了 X^2 是 m^2 的倍数, 故 X 是 m 的倍数. 记 $X=mp'$, $Y=mq'$, 我们得到了三元组 $(p',q';m')$.

为了把 m 做小, 我们看出可在模 m 的同余类中选取一个 x 使得 $x<\sqrt{N}<x+|m|$; 如果这时有 $\sqrt{N}+x<0$, 那么我们就会有 $2\sqrt{N}<|m|$; 如果因此而假设 $|m|<2\sqrt{N}$, 则这种情形便不会发生, 从而有

$$0<N-x^2=(\sqrt{N}-x)(\sqrt{N}+x)<2|m|\sqrt{N},$$

因此也就有 $|m'|<2\sqrt{N}$. 现在我们可以将这同一个过程用于 $(p',q';m')$ 得到了 $(p'',q'';m'')$ 等等. 由于这些 $m,m',m'',\cdots$ 有界, 它们自身一定会重复; 或许这就是给以 "轮转" 法名字的来源吧.

这需要许多考量. 首先, 我们刚刚给出了证明的那些事实对于印度人来说可能只是从实验上得知的; 没有任何东西表明他们对于这些事实有所证明, 哪怕是部分的. 其次, 为了要完成 *cakravāla*, 必定要有一个起点; 他们总是一成不变地选取 $(p_0,1;m_0)$ 为这个元, 其中 p_0^2 是从上或下最靠近 N 的平方数; 于是容易看出这时 $|m_0|<2\sqrt{N}$. 这样一来, 因为已有 $q_0=1$, 当然在第一步就不需要 *kuṭṭaka* 了; 然而也就在以后的每个运算中不再需要了, 这是因为, 在上面的记号

下, 我们有 $p'-q'x=-qm'$, 故而在下一步就必须取 $x'\equiv -x \pmod{m'}$. 十分奇怪, 这似乎并没有被印度的作者们注意到 (一直到十六世纪前甚至也没有引起后世的评论者的注意); 他们没有提及它, 并总是向 *kuṭṭaka* 去查询 x 的选取, 尽管他们的充足的数据容易使他们相信没有必要这样做. 再者, 印度人对于在模 m 的同余类中选择 x 的描述并不全像我们前面所表述的那样, 这是因为这个法则是把 $N-x^2$ 做 "小" (即, 在实际操作上要尽可能的小), 而是, 如上下文表明的那样, 在模 m 的绝对值的类中选择; 换句话说, 当 x_1^2-N 出现小于 $N-x^2$ 时, 应该以 $x_1=x+|m|$ 替换 x. 可以证明, 当出现这种情况时, 这样做的效果仅仅是缩短了一点这个过程而已. 最后, 我们被告知进行迭代的过程一直要到找到一个 "加元" m 是 $\pm1,\pm2,\pm4$ 之一才为止, 然后再应用 *bhāvanā* ("复合")法则, 即对于那种情形的婆罗摩笈多的过程. 实际上, 这只不过是条捷径而已, 因为可以证明以直接的方式应用 *cakravāla*(轮转法) 将必定引向所要的三元组 $(p,q;1)$; 尽管从数值计算的观点看, 这条捷径十分有效, 但它破坏了这个方法的 "轮转" 特性, 不然的话, 就会出现这些 "加元" $m,m',m'',\cdots$ 自身周期性的重复, 它对应于 $\sqrt{N}$ 的连分式的周期性 (参看第三章,§12).

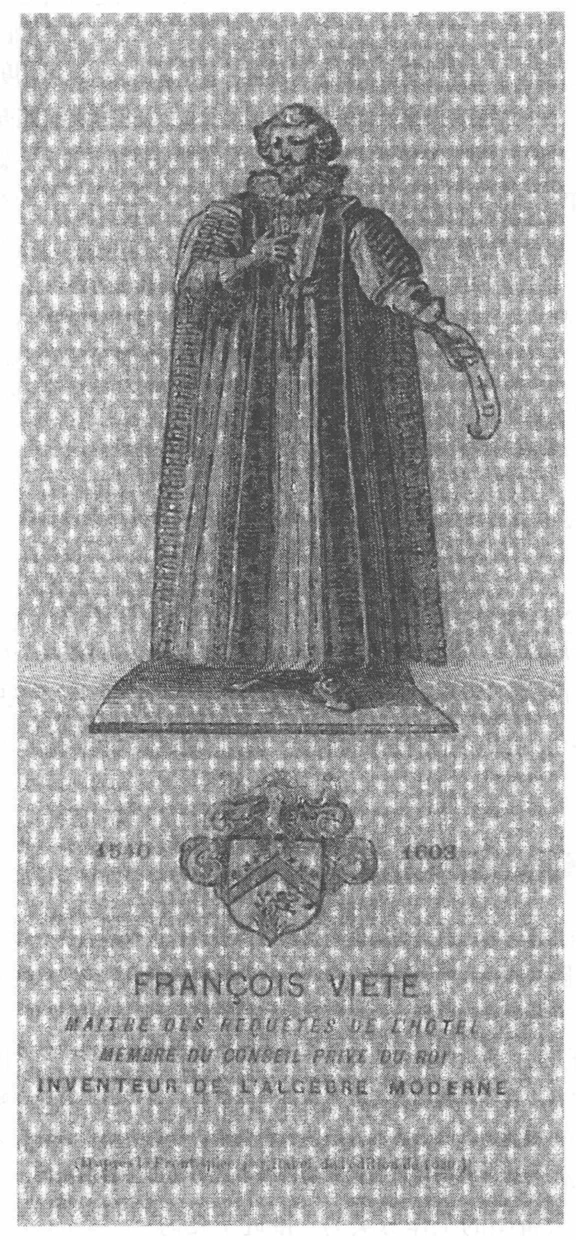
当然, 对于印度人来说, *cakravāla* 的有效性可能只不过是一个实验性的事实, 它基于对极大量特殊情形的处理, 其中有一些相当复杂并涉及 (无疑使他们感到高兴) 十分大的数. 像我们将要看到的那样, 费马是第一个感觉到需要有一个一般性证明, 而拉格朗日则第一个发表了一个证明. 但是, 发展出 *cakravāla* 并将其成功地应用于诸如 $N=61$ 或者 $N=67$ 如此困难的数值情形, 也并非是平庸的成就.

§1.10 丢番图与丢番图方程

当费马开始他作为数论学家的生涯时, (撇开欧几里得不谈) 他极少拜读其他的著作, 但要除去巴歇所编撰的关于丢番图的书, 以及韦达在他 1593 年的《*Zetetica*》中关于丢番图的那一大部分的熟练而精彩的叙述.

像他后来有机会观察到的那样, 不管是韦达甚至还有丢番图都不是真正的数论学家. 1657 年, 在他质疑英国数学家 (*Fe.*II,335) 时写道, "数论处理的是整数, 而从另一个角度看, 丢番图处理的是有理数, 韦达则将丢番图的工作推广到了连续的量, 这清楚表明它并不真正属于数论". 费马紧接着把韦达的工作归之为 "几何", 而将丢番图的工作分类为 "接近于几何".

从我们现代的观点看, 事情有点不太一样. 首先, 由于丢番图如此多的工作及韦达的甚至更多的工作在任意域上仍旧成立, 我们会将其主要地分类到代数; 当然, 韦达的代数无论从记号上还是从内容上都是远为先进的, 比起丢番图的来


1540
1603
FRANÇOIS VIETE
MAITRE DES REQUETES DE L'HOTEL
MEMBRE DU CONSEIL PRIVE DU ROI
INVENTEUR DE L'ALGEBRE MODERNE

韦达像 (雕版画)

更加接近我们. 其次, 在有理数与整数之间的区别也并非像前面所引述的费马所说的那样一清二楚; 正如他非常清楚知道的那样, 当处理齐次方程时, 这种区别并不适用. 再者, 我们不久就可以看到, 在丢番图那里以及在韦达的《*Zetetica*》中的许多内容, 按我们的观点看, 应归属于代数几何. 进一步说, 现代的发展使得我们已能够更好地理解函数域与数域之间的类比性 (莱布尼茨与欧拉在某些场合也已朦胧地感觉到这点), 表明在以有理数解一个问题与在有理函数域中解一个问题有时并没有什么差别.

当人们试图将在丢番图中出现的问题和方法进行分类时, 所有这些观点都显示出了重要性. 他传承给我们的著作由差不多二百个问题组成, 其中每一个都要求求一组给定方程的正有理数解. 丢番图每次对一个未知量以及它的各个幂 (具正或负的指数) 都给出了记号, 但对其他的则无; 如果在一个问题的讨论过程中还必须再讨论一个辅助问题, 则把同一个记号用到这个新的辅助未知量上, 用过之后便予放弃. 所给数据常常包含一个或一个以上的常数; 由于它们不能以字母代表, 不得不给它们指定任意的数值值; 另外, 通常总期望解含有与问题, 或者至少与求解的方法相匹配的尽量多的参数, 然而在问题出现之时便已不得不对它指定了数值的值; 如果后来证明它必须满足某些条件而原来的选择却并不满足的话, 那么以后就可将其改变 (这是显然由最早用在线性问题的著名的老的试位法 (*regula falsi*)). 偶然也会讨论一些不甚完整的问题, 有时将其作为一个引理, 而该引理包含了以后必定会起未知元作用的参量; 称这样的显式参数解为 "不定解"(参看, 譬如 *Dioph.*IV,19, 这个词在那里有定义). 丢番图当然留意到了无理量的存在; 有时候, 当某些参量的初始选取将会导致未知元这种值时, 他便会以 "该未知元变成了无理数" 的话予以舍去 (参看, 例如 *Dioph.*IV, 9).

要描述出这些问题在全书中或在其每本书中前后安排的特性不是件容易的事; 其实也无此必要, 因为我们不能肯定这种安排就一定能够回溯到丢番图 (或者是该选集的无论哪一个原作者或编撰者) 那里. 至于这个方法, 它在于 (根据达朗贝尔*27 以其固有的明晰风格将它放进 1750 年的《百科全书 (*Encyclopèdie*,tome IV,p.1014)》的文章 " 丢番图" 中)"对未知量进行这样的变换, 使得将该问题简化为一个未知量的线性方程"["*manier tellement les inconnues ou l'inconne que le quarré et les plus hautes puissances de cette inconnue disparaissant de l'equation, et qu'il ne reste que l'inconne au premier degré*"]. 但是, 某些类型的方程以极高的频率出现, 我们现在就要对它们进行检验. 最好先将它们用现代的术语加以描述 (参看第二章 §14–§15 及附录 II).

最终, 大部分问题可化成在一条亏格为 0 或 1 的代数曲线上, 找出一个具有

---

*27 Jean Le Rond d'Alembert, 1717—1783, 法国数学家, 是研究微分方程的先驱者并将其应用到物理中; 他研究了流体的平衡和运动理论.

正有理坐标的点的问题, 而这条曲线由一个或一个以上的方程定义. 如上所述, 这些方程的系数不得不以数值的方式陈述, 但它们经常也包括了参量, 从而意味着这个求解的方法应该赋予未知量以由这些系数有理表示的值. 当然, 只要可以使用一些现代的代数记号, 譬如韦达的, 这个断言就容易得到证实.

现在已有可能区分两种主要的情形:

I. *亏格 0 的情形*: 不管它是仿射的还是射影的, 这样一条曲线必须至少有一个有理点, 这要么是显然的要么是容易找到的. 只要这个 "看得见" 的解位于仿射空间中且已满足了所有要求的附加的条件 (譬如一些不等式), 在丢番图的眼里便不会有任何问题. 如果不是如此, 那么观察到在这样的曲线上有理点是处处稠密的则是至关重要的. 韦达在特殊情形圆 $X^2+Y^2=a^2+b^2$ 已显式地将其表出 (*Zet*.IV,5= *Op*.pp. 65–67); 似乎丢番图也已注意到此, 然而他也没有一个一般的方法来表达它, 但他用了一个特别的词 ($\pi\alpha\rho\iota\sigma\acute{o}\tau\eta\varsigma$, 依照克西兰德和巴歇的用法, 费马将其翻译为 *adaequatio* 或 *adaequalitas*) 来表示对于一个已知问题以其有理解来近似一个已知数的方法 (参看, 例如 *Dioph*.V, 11 和 14). 在丢番图处经常出现的亏格 0 曲线的典型情形是由平面二次曲线 $AX^2+BX+C=U^2$ 给出的, 其中或者 A, C 或者 (如同在 *Dioph*. VI. 12 的第二个引理中那样)$A+B+C$ 为平方数. 于是如果 $A=p^2$ 或 $C=q^2$ 则令 $U=pX+q$; 符号自然按每种情形的要求进行调整.

II. *亏格 1 的情形*: 这条曲线必须至少要有一个 "看得见" 的有理点和一个 "看得见" 的有理偶对; 例如, 方程

$$AX^4+BX^3+CX^2+DX+E=U^2,$$

其中 A 或 E 为平方数便是这样的 (参看, 譬如 *Dioph*.VI,10). 更经常遇到的是具有一个 "二重方程" $P(X)=U^2, Q(X)=V^2$, 其中 P 和 Q 有以下形式:

$$P(X)=AX^2+BX+C, \qquad Q(X)=A'X^2+B'X+C'.$$

如果 P 和 Q 在射影直线上有一个公共根, 例如, 当 $A=A'=0$ 或者当 $C=C'=0$ 时, 它们便在 (X,U,V)- 空间中定义了一条亏格 0 的曲线; 如果不是这样, 则其定义了一条亏格 1 的曲线. 在丢番图中总是反复考虑 $P-Q$ 或有时也考虑更一般的对于适当 m,n 的 m^2P-n^2Q, 使它们在射影直线上具有两个有理零点的情形; 例如当 $A=A'$ 或者 $C=C'$ 便属此种情形. 于是我们便有 $P-Q=LM$, 其中 L, M 为有理因子, 而二次式 $P-Q=U^2-V^2$ 具有两个直线的有理系

$$U\pm V=tL, \quad U\mp V=t^{-1}M.$$

其中任一条直线与 $P=U^2$ 的交给了我们一个有理偶对; 如果 A 和 A', 或者 C 和 C' 都是平方数, 我们甚至得到了两个有理点. 亏格 1 曲线的一般理论可清楚

告诉我们, 由以上这些如何进一步推导出其他的点来. 丢番图令

$$U = \frac{1}{2}(tL + t^{-1}M),$$

而后调整 t 的值使得 $P = U^2$ 具有一个有理解的办法也得到了同样的结果 (参看, 譬如 *Dioph.*III, 17 或 IV,23). 平面三次曲线也可归入到这个相似方法的范围内 (参考, 譬如 *Dioph.*IV,24). 但是应该注意到, 丢番图对于他的方法从来没有做过其他的应用, 从而没有使他能找到要求满足一些不等式的解. 于是, 我们不得不等到讨论费马对此相同问题的处理时再更仔细地考虑它 (参看第二章,§15).

§1.11 丢番图及平方和

尽管前面的叙述似乎充分地涵盖了丢番图现存的几乎全部的工作, 但人们还会在此遇到几个使人感到迷惑的暗示, 它可能提示了一些完全不一样的课题. 一个问题 (*Diph.*V,9) 是要求找一个可以表达为 $x^2 + y^2$ 的数 $A = 2a + 1$, 满足附加条件 $x^2 > a$, $y^2 > a$; 按照 *Dioph.*II,9 的理由, 或是由于如下事实, 后面这个条件是可以忽略的: 这个事实是说, 如果一个圆的半径为有理数, 则该圆上的有理点处处稠密 (参看*supra*,§X). 另一方面, 我们所拥有的*Dioph.*V,9 对此没有做出什么有意义的解释, 显然误入歧途, 它对 a 定出了一个条件 (说它不应该是个奇数) 似乎还涉及 A 的素因子. 因此其至少说明 a 是一个整数 (而通常丢番图仅仅假定数据是有理的). 在这个问题的解中, 已知 a 的值为 6 , 从而 $A = 13 = 2^2 + 3^2$, 因此解 $x = \frac{257}{101}$, $y = \frac{258}{101}$. 在 *Dioph.*V,10 中, 有一个类似的问题但具其他的附加条件并且 $A = 9$. 而在 *Dioph.*V,11 中我们有 $A = 3a + 1$ 的相应问题而方程则为 $A = x^2 + y^2 + z^2$; 到了此刻书的内容才表现得条理清晰而意思明确起来, 它只不过是在限定 a 不是 $8n + 2$ 的形式罢了, 就是说, A 不是形如 $8n + 7$ 这样的数. 总之必须在 *Dioph.*VI,14 中添上陈述说, 15 不是两个平方数的和以及 "因而" 方程 $15x^2 - 36 = y^2$ 在有理数中无解; 但对于这些并非完全平凡的陈述, 它没有给出任何解释. 最后, 如巴歇所观察到的那样, 问题 *Dioph.*IV, 29 和 30 认为任意整数 (或者, 大概指的是有理数吧) 可以写成四个平方数之和; 这并不会令我们感到惊奇, 因为对在那些问题中所选的数据而言这的确是对的.

还有一个使人想知道的问题是, 丢番图或他的前人关于将整数分解为 2, 3, 或 4 个平方数和的方面究竟知道多少; 当然, 他们的这方面的知识可能只是实验性的结果. 在费马开始着手研究这些问题后不久, 他就看出运用模 4 或 8 的同余式相当容易地便能证明某些分解是不可能出现的; 因此可以看出, 譬如当 A 形如 $4n + 3$ 时便不能写成 $x^2 + y^2$ 的形式, 当它形如 $8n + 7$ 时则不能写成 $x^2 + y^2 + z^2$ 的形式 (参看第二章 §5). 尽管在丢番图的任何地方都没有发现过

这样的论证, 但也不能因此就说他们违背了希腊算术的精神. 只要没有迄今仍不为人知的资料的突然发现, 所提出的这些问题便不会有答案.

§1.12 丢番图的复苏: 韦达与巴歇

对于一个十六世纪的数学家来说, 丢番图是一个不易解读的文本, 而且对于必须要去看拉斐尔・邦贝利和克西兰德写的东西才能了解被重新发现的丢番图的这种观点, 他们完全不以为然. 邦贝利大约是在 1570 年, 为了自己的使用, 在罗马阅读并翻译了丢番图, 而后则将其放进了他 1572 年意大利文的著作《代数》中; 克西兰德则是第一个努力做全本翻译的人, 于 1575 年在巴塞尔出版了他的成果. 当然, 这类工作的实质性困难随着可用手稿文本的相对缺少而大大增加. 实际上, 对于所有希腊的经典作者的情形而言都属此例. 他们的著述全都从一个手抄孤本 (所谓的 "原型 (archetype)", 但现已不知所踪) 得来, 而这个孤本却已被在转抄中的讹误和遗漏所损害. 在丢番图的情形, 其中最糟糕的是数值上的错误. 无疑抄写是由专业的抄写员完成的而不是数学家; 或许幸亏如此, 如果是数学家的话恐怕会更糟糕.

第一位要说的翻译者是 Holzmann, 他将自己的名字按希腊风格叫成克西兰德 (Xylander); 他是个人文学家, 一个古典文学学者, 但将代数学作为业余爱好. 邦贝利则是位忙碌的工程师, 他设计运河, 改造湿地, 并且把他的慷慨的雇主和资助人梅尔菲 (Melfi) 主教所给的几乎所有的休闲时间都奉献给了数学. 当他把丢番图的资料插进他的《代数》的 "书" III 时, 他的意图似乎仅仅是用它来充实他至少是十年前所写的一篇文稿. 作为代数学家, 他自身的能力体现在其他方面, 譬如在他的 "书" I 中对复数的 (相当现代的) 处理上, 还有在 "书" II 中的三次和双二次方程的理论上. 另外一位是韦达. 尽管他所接受的是律师的教育, 并以此作为了他大部分生命中的职业, 但他把自己首先看作一个数学家, 他的同时代的人也持同样的看法. 在他 1591 年的《分析方法入门 (*In Artem Anallyticem Isagoge*)》的序言中他用了 "*Ars nostra*(我们的艺术)" 来称呼数学, 这本《*Isagoge*》是树立他为那个时代最伟大代数学家声誉的一系列著作的第一部. 在他即将透露他的发现时, 他形容这个发现是 "纯金", 又补充道 "不是炼金术士的金, 它立刻会化为一道青烟而消失, 是真正的金属, 是从由龙把守的矿山中挖掘出来的". 紧随着他的《*Isagoge*》之后又有了他 1593 年的《*Zetetica*》*[28], 在这里有着许多丢番图提供的含金矿石; 那么, 他前面所说的 "纯金" 对他而言

*[28]是指一种分析问题的方法, 即把一个问题转化为连接未知量与各已知量的方程的过程. 参看 J.Katz 的《数学史通论 (*A History of Mathematics——An Introduction*)》, 中译本, 高等教育出版社.

已不是什么了不起的事了; 他的目的是要展示这个新代数的威力和范围; 所以在运用丢番图时他的全部注意力都集中在实现这个目标上了. 而这里, 正如费马完全看出的那样, 在丢番图那里出现的哪怕一点点数论方面的东西都已被丢弃殆尽了.

因此这仍然是一个巨大的任务, 它等待着未来丢番图的编撰者们、翻译家们、评论家们去完成，甚至在他们的先行者们做过的所有的工作之后依然如此. 如同费马的儿子塞缪尔在 1670 年的《丢番图》的序言中表达的那样 (无疑反映了他父亲的情感, 或许就是他自己的话):

“邦贝利在他的《代数》中的行为不是作为一个丢番图的翻译者, 因为他把他的问题与这位希腊作者的混在了一起; 韦达也不是的; 因为他开创了通向代数的一条新路, 他所关心的是将他自己的发明带进大众瞩目的中心, 而并不是要做高擎丢番图思想的火炬手. 因此才需要克西兰德的不懈劳作和巴歇的令人羡慕的睿智, 这给我们提供了丢番图的伟大著作的翻译和诠释.”

C. G. 巴歇, 德 · 梅齐里亚克阁下 (Claude Gaspar Bachet, sieur de Méziriac) 是一位具中等财力的乡绅，具有对经典的鉴赏力，但不是位数学家. 他多多少少显示出对某种数学游乐和谜语的兴趣，这是些在希腊文的诗画等汇编的《选集 (*Anthology*)》中的许多 epigram (警句) 那一类的东西, 以及像在中世纪和文艺复兴时代的文本中的, 或者像现今我们报纸和杂志中谜语专栏中那样的东西. 1612 年, 他在里昂出版了一本这类谜语的集子, 书名是《*Problèmes plaisants et délectables qui se font par les nombres* (与数相关的令人愉悦和舒心的问题)》. 如书名所示, 他于是走到了数论, 走到了丢番图. 后者必定在该书出版的 1621 年前已占用了他多年的时间; 在看到该书已出版后, 他退隐到他的乡村家中, 结了婚, 除了准备他的 1621 年的《*Problèmes*》的第二版, 显然放弃了所有的数学活动, 在第二版中他打算加进一篇关于算术的论述, 但这从来也未问世 (参考 *supra*,§IV). 附带说一下,《*Problèmes*》赢得了如此的欢迎，使得它们享有甚至直至本世纪的连续不断的再版.

塞缪尔 · 费马对巴歇的赞扬绝非夸大其词. 一个文献工作者总是想要弄清那些手稿中许许多多已损坏段落的意思; 而克西兰德却常常不能做到这点. 巴歇则总是孜孜不倦地盯着克西兰德的翻译和注释的缺点, 同时也自然而然地赞扬了他自己的优点. 他甚至冒大不韪地以轻视的口吻提到韦达的代数方法, 而他对此既不会欣赏也弄不懂; 但这并不妨碍他不声不响地从韦达的《*Zetetica*》(*Zet.* IV,12,15,18,20 = *Op.* pp.71,73–75) 中提出两首 “porism” (III.11 和 III.14) 和一些关于立方的重要问题 (在他对 *Dioph.* IV,2 的评注中). 不过, 他所做的这一切却造福于后人, 特别对费马, 这为他们提供了一份丢番图的可信赖的文本, 以及在数学上可靠的翻译与注释. 甚至他对于新代数的不理解最终也可以说成是有



费马像 (雕版画)

利于数论. 他这样做无疑使得他写出了超大量的注释和 “porism”, 并且在它们前面都写了前言, 但这些前言中则充斥了大量可笑的笨拙证明. 与此同时, 由于他的主要兴趣是数论而非代数, 他总是一成不变地把重点放在文本里更具有真正算术特性的方面, 而其中更突出的则是关于将整数分解为平方和的所有问题 (参看 *supra.* §XI). 他寻求一个整数为两个或三个平方数和的条件, 从丢番图那里摘取出一个整数可表为四个平方数和的猜想并寻求证明.

大幕已可升起; 舞台业已搭好. 费马也可以出场了.

第二章　费马和他的信件

§2.1　生平

我们现在来讲一下费马那看起来并不平坦的一生. 他出生在法国南部的一个小城 Beaumont de Lomagne 的一个富裕的中产家庭, 离朗格多克 (Languedoc) 省的图卢兹 (Toulouse) 市不远. 他的母亲 Claire de Long 属于称为 “noblesse de robe” 的法国南部的贵族家族, 这个称呼表示她的家庭中曾有一个以上的成员通过执掌行政权而被授予贵族头衔. 他于 1601 年 8 月 20 日受洗礼, 命名为皮埃尔 · 费马 (Pierre Fermat). 在 1631 年前有一段时间, 或许几年, 他是在波尔多度过的. 1631 年 5 月 14 日他被接受进入 “Parlement”, 即在图卢兹的省高等法院, 头衔为参事 (councilor), 这是他一直到死的终身职位; 因为这个原因, 从此他被称为费马大人 (Monsieur de Fermat), 他的同代人也都这样称呼他. 1631 年 6 月 1 日, 他与 Louise de Long 结婚, 她是他母亲家的一个远房表亲. 他们有两个儿子三个女儿; 大儿子塞缪尔成了一个公职人员, 像他父亲一样, 是图卢兹高等法院的一个参事; 他的弟弟则领了圣职, 成了卡斯特雷 (Castres) 大教堂的教士; 姐妹中一个结了婚, 另两个成了修女. 费马的职业生活分成为两部分, 一部分在图卢兹, 是他的主要居住地, 另一部分则在卡斯特雷, 这里是图卢兹高院的 “ Chambre de l'Edit” 的场所; 这里办理有关天主教和本省的新教社团之间的司法诉讼[1]. 在一次公务轮转时费马逝世于卡斯特雷, 这是 1665 年的 1 月 12 日.

[1]费马的许多涉及其职业生涯的信件已得到保存 (*Fe.*11,letters LI,LIV,LV,LIX,LXIV,LXV, LXVI,CXI, 以及*Fe.*IV,15–22; 参看 *Fe.*III,505). 也可参考 P.Chabbert 的出色研究《费马在卡斯特雷 (Ferma à Castres)》,*Rev.d'Hist.des Sc.*20 (1967),pp.337–348.

费马显然喜爱优秀的经典教育; 他十分精通拉丁、希腊、意大利和西班牙文, 他以多种文字写诗的本领得到了广泛的赞扬, 这一本领也传给了他的儿子塞缪尔. 他收集原稿; 他建议紧急地寻求对希腊文本的校订. 有着这样兴趣的十七世纪的绅士自然会想到造访意大利; 对于费马而言, 那个国家活跃的科学生活, 还有那里出现的诸如伽利略、卡瓦列里*1 (B.Cavalieri)、里奇 (Ricci)、托里拆利*2 (E.Torricelli)等科学界人物应该给予了他额外的吸引力. 确实他的一些最好的朋友进行了这种旅行并在途中拜访了意大利的科学家们: 有 1634 年的德・卡尔卡维*3 (Pierre de Carcavi), 1635 年的博格兰德*4(Jean Beaugrand), 以及 1644 年和 1645 年的梅森. 但没有迹象表明他自己曾想到过要追随他们的后尘. 在 1636 年给梅森的最早的一封信 (*Fe*.II,14) 里, 他有点含糊地说道 "找个机会到巴黎去待上三四个月", 他说这会给他一个写出他关于一些几何课题的思想的机会; 但这并没有成为现实. 在其生命后期的 1660 年, 他对帕斯卡表达了想要会见他的热切愿望; "由于他的健康状况和帕斯卡的简直一样差" 这必将发生在 "克莱蒙*5 和图卢兹居中的某地" (*Fe*.II,450); 帕斯卡也出于健康的理由 (*Fe*.II,450–452) 没有进行这次旅行, 的确, 在那些日子里对一个病人来说这是一次需要付出巨大努力的事. 同年, 听到惠更斯正在巴黎 (*Fe*.II,452), 费马向他保证说, 只要健康允许他旅行他就会到那里去会见他; 显然他希望惠更斯能领会到他的暗示来拜访他自己, 他通过卡尔卡维与惠更斯已有过多次关于科学方面的通信 (*Fe*.II,322,328,431,446); 即便如此, 他的期待也没有实现.

费马最终到死也不曾[2] 有胆量去到比从家到波尔多更远的地方过. 像他的信件所表明的那样, 他的休假通常是 "*à la campagne*", 即在他乡下的房子里度过的.

没有资料告诉我们费马是什么时候变得对数学有兴趣的, 但这必定出现在当他二十几岁, 逗留在波尔多的时候. 在那里他遇见了德・埃斯帕内特 (Etienne d'Espagnet), 他自己是个公职人员同时也是个公职人员的儿子; 他们成了亲密的朋友 (参看, 譬如 *Fe*.II,71,105,136). 埃斯帕内特比费马大五岁左右, 爱好数学, 人们喜欢把他想成是第一个认识到费马的天赋的人, 并给了他一些鼓励, 而年轻

[2]或者说几乎没有过; 在 1631 年他被列在有奥尔良 (Orléans, 法国中部城市 —— 译注) 的取得法律学位的名单上; 但这或许是在缺席情况下取得的.

*1 1598—1647, 意大利数学家、神学家; 有几何学方面的著作, 发展了完整的不可分量理论, 并有以其名命名的 "卡瓦列里原理".

*2 1608—1647, 意大利科学家, 曾随伽利略学习, 制作过实质性的真空并发明了气压计, 在数学上也有关于无穷小量等方面的建树.

*3 1600?—1684, 法国人, 业余数学家, 以与其他数学家的通信而知名; 与费马在图卢兹为同事; 参看本节后文.

*4 1600?—1640, 法国数学家, 出版过关于刚体力学和数学方面的著作, 参看本节后文.

*5 帕斯卡的出生和居住地.

人没有这些鼓励是不行的. 他告诉费马, 在他的收藏中有韦达没有发表过的著述 (*Fe.*II,133); 推想起来, 他大概有一套多少算是韦达著作全集的东西吧, 在那个时代那么一套东西是很难得到的; 显然费马仔细地研读过它们, 这是在他学术生涯的早期, 远在它们在 1646 年因 F. 舒腾 (van Schooten) 出版了《*Vièta Opera Mathematica*(韦达数学文集)》而能普遍获得之前. 至于埃斯帕内特, 他是费马的终生挚友, 不仅仅保持了与他的私人关系而且也一直保持了对费马在数学上进展的强烈兴趣 (参看 *Fe.*II,221). 1646 年, 为了把费马 "从贝尔热拉克*6那里拽出来" 以参加在波尔多的一个三日聚会, 梅森不得不让埃斯帕内特去对费马施加压力 (*Fe.*Supp,136, 注 (1)).

韦达于 1603 年在巴黎逝世; 在这个世纪的二十和三十年代, 他的一些崇拜者们关注到他的方法的传播问题; 他们的努力以前面所提到的 1646 年的《文集》作为终结成果. 在这个小集体中有博格兰德, 这位 " 奥尔良的 H.H. Gaston 数学家 (*mathematician to H.H. Gaston d'Orléans*)" (不知有点什么意思), 他后来就任公职, 为宫廷秘书 ("secrétaire du Roy"; 参看 *Fe.*IV,22, 注 (1),2°); 像在那些日子里的科学家或热衷于科学的人士一样, 他与著名的梅森神父有联系, 而他自己并非严格意义下的数学家, 但他却与梅森合作注释了韦达 1631 年版的《*Isagoge*》和《*Notae Priores*》*7; 后一本书从来没有出版过, 而前一本已经绝版. 有鉴于此, 当我们发现博格兰德在 1630 年一封给梅森的信 (*Mers.*II,515) 中提到了 "这些波尔多大人们 (*ces Messieurs de Bordeaux*)", 并写道他已经寄给他们好些力学问题, 要说其中包括了埃斯帕内特似乎不算牵强; 它也完全有可能包括了费马, 只要那时博格兰德已经知道了他的名字. 但有一点是可以确认的: 在随后的年月中, 至少直到 1638 年在费马和博格兰德之间进行了许多关于数学议题的交流 (参考 *Fe.*II,4–5,20,28,72,94,105,106,133). 在他 1635 年到意大利的旅行期间, 博格兰德对意大利的科学家们热切地讲到了费马 (参看 *Fe.*II,26, 注 (1)) 并向他们展示了费马的一些结果 (参看 *Fe.*Supp,99), 还可能 (根据同代人的暗示) 把某些荣誉归于了自己 (参看 *Fe.*II,26, 注 (1),*Gal.*XVI,328,345, 和 *Fe.*Supp,113,114).

博格兰德于 1640 年逝世; 还不清楚是否他会见过费马, 但有迹象表示后者对他的热情关注 (*Fe.*II,4–5) 在 1640 年之前就已经冷却了 (参看 *Fe.*II,111,133, 或许还有 II,207). 费马与卡尔卡维之间的友谊持续了更长久，后者在 1632 年成了费马在图卢兹高等法院的同事，并在 1636 年前都一直在那里. 之后他转移到了巴黎，在那里他对于以梅森、E. 帕斯卡*8 和罗伯瓦尔*9(G.P.de Roberval) 为中心的那个学术圈子变得十分熟悉. 费马与这个团体成员的学术通信便是由一

*6Bergerac,1619—1655, 法国作家, 著有两部探访月球和太阳的科幻小说.

*7见第一章 §6

*8B. 帕斯卡的父亲，在科学委员会任职.

*91602—1675, 法国数学家, 对于曲线的几何, 特别是摆线, 有重要贡献.



FRANCISCI VIETÆ

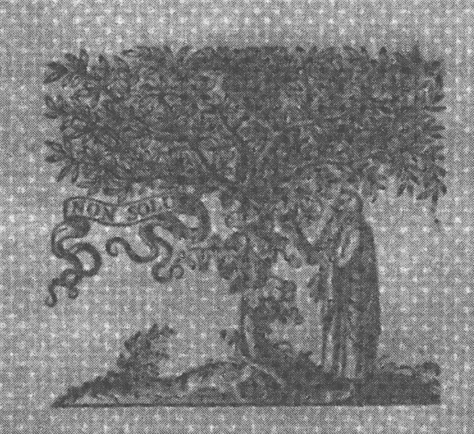
OPERA

MATHEMATICA,

In unum Volumen congesta, ac recognita,

Operâ atque studio

FRANCISCI à SCHOOTEN Leydensis, Matheseos Professoris.



LUGDUNI BATAVORUM,

Ex Officinâ Bonaventuræ & Abrahami Elzeviriorum.

CIƆ IƆ C XLVI.

《韦达数学文集》的扉页

封给梅森的信开始的, 这发生在卡尔卡维到达巴黎后不几天的时间里. 自此直到 1662 年前后这样的通信就再也没有停止过, 之所以停下来, 或许是出于健康不佳的原因 (参看 *Fe*.II,450) 让 "他的几何进入了休眠" (*Fe*.II,485). 这封信的相当重要的部分被保留下来了; 无疑它给费马提供了他从事数学事业的主要外部动机, 这是因为他与一个数学家曾经有过的最紧密亲身接触 (除了博格兰德的假想式的拜访外) 就是前面所提到的与梅森的那次三日聚会, 它也很可能不是如此描述的那样. 在梅森于 1648 年逝世后, 卡尔卡维取代了他作为在当代从事科学的人们间的媒介人的角色; 据卡尔卡维所说, 在 1656 年他真诚地向惠更斯介绍时说自己是个 "对数学不甚精通但却非常热爱" 的人 (*Fe*.IV,118). 拉罗维尔神父 (Father Lalouvère) 是图卢兹地方耶稣派学院的数学教师, 他对于费马也没有发挥多少作用; 在 1658 年举行了一次著名的关于摆线整体计算的有奖竞赛*10(参看 *Fe*.II,413,430), 拉罗维尔这次不愉快的参赛被帕斯卡 (非相同教会教友) 在 1658 年他的"*摆线的历史*(*Histoire de la Roulette*)" 中兴高采烈地取笑了一通. 但是我们还是要感激拉罗维尔, 因为在他 1660 年出版的关于摆线的书的附录里有费马的一篇也是唯一被他允许发表的作品, 这是关于求曲线长的匿名论文 (*Fe*.I,199–254). 对于这方面, 还必须提到霍夫曼 (J.E. Hofmann) 在 1943 年发现的八页匿名文章[3], 它们是附加在弗莱尼柯关于 "佩尔方程" 及其他专题的一本极其少见的小册子上的; 它们由一封给弗莱尼柯和一封给迪格比*11 (Kenelm Digby) 的私人信件, 它必定是没有得到费马首肯而发表的, 因为甚至在费马的儿子准备 1679 年的《*Varia Opera*》时显然也还不知道它.

在费马活着的时候确实在若干场合都提出过出版他的著作的问题. 如我们已经知道的 (第一章 §1) 那样, 他曾表达过要以书的形式写出他在数论上发现的坚定决心 (*Fe*.I,305,Obs.XVIII). 1654 年他曾邀请卡尔卡维和帕斯卡合作一项雄心勃勃的计划: 他希望他们协助他准备出版他的巨大的数学工作, 而帕斯卡将单独负责数论部分, 因为费马已完全放弃把它们完整写出来的努力了 (*Fe*.II,299). 这个计划最终归于零, 但不管费马相当低落的情绪和在他的 1659 年 8 月的通信中 (*Fe*. II, 436) 表达的对于自己算术发现 (他称它们为 "*mes resveries*") 所进行的简明叙述中的令人气馁的结论, 卡尔卡维还是在 1656 年向惠更斯提出了这件

[3] J.E.Hofmann, Neues über Fermats zahlentheoretische Herausforderungen von 1657, *Abh.d. preuss.Akad.d.Wiss.* 1943–1944,Nr.9,pp.41–47.

*10 该竞赛是由帕斯卡发起的, 他提出了一组关于摆线的具挑战性的问题, 并许诺对最好的解答给予一等和二等奖. 罗伯瓦尔是评判人之一. 这个竞赛只收到了拉罗维尔和沃利斯的两份解答. 帕斯卡和罗伯瓦尔决定这两个参赛者都不应得奖. 取而代之的, 帕斯卡发表了自己的解答连同一篇短文 "摆线的历史" 表明在罗伯瓦尔与托里拆利的优先权的争论中站在了前者的一边. 这引起许多人的不快.

*11 1603—1665, 英国廷臣, 海军军官, 外交家, 自然哲学家.

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,

ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT *Senatoris Tolosani.*

Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.



TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.

M. DC. LXX.

《丢番图》的扉页

事 (*Fe*.IV,120), 而后又在 1659 年再次提出 (*Fe*.IV,126). 最终在他身前对此毫无作为.

实际上在那些年月里, 一个数学家要将一项工作交付出版绝非易事. 一个还说得过去的出版人, 他必须受到作者或者是熟悉作者风格与记号的某人的严密地监督, 但这还不够. 极其频繁发生的是, 一旦书面世了, 它就成了无穷无尽的激烈论战的靶垛. 那么当出版问题提出时, 人们还会对费马首先要坚持匿名感到奇怪吗 (*Fe*.II,106,299)? 同时, 显然在为了出版而写出证明上他总感到了非同寻常的困难; 只要涉及数论, 这种尴尬局面就近乎是一种麻痹状态, 因为对他来说, 这里没有任何古代或现代的范例可以遵循.

费马从来没有对保存他与其通信人的信件复本的问题烦心过 (参看, 譬如 *Fe*.II,218). 因此, 在他身后, 命定要由他的儿子塞缪尔去竭尽全力收集他父亲散落各处的残留手稿. 他以 1670 年的《丢番图》开始着手, 这是巴歇 1621 年的《丢番图》的一个重印本, 其中他插印了费马在他自己的那本的边白上草草写下的笔记的完整内容. 作为巴歇过去的朋友、第戎 (Dijon) 的一位数学教师的耶稣会教士 J. 德 · 比利, 写了一篇 36 页的文章《*Doctrinae Analyticae Inventum Novum*》; 这篇文章是根据费马的一系列信件写成的 (现在除了一封 1659 年的早期信件外, 其他的均已遗失: *Fe*.II,436–438); 它较详细地叙述了费马处理亏格 1 的丢番图方程 (参看第一章 §10, 以及下文的 §15) 的方法, 并自然地赞美了费马优于丢番图、韦达和巴歇的那些地方. 随这本书之后又有了《*Varia Opera*》, 它的主体组成包括了费马关于几何、代数、微积分方面的著述, 连同与梅森、罗伯瓦尔、E. 帕斯卡、弗兰尼柯、B. 帕斯卡、卡尔卡维、迪格比、伽森迪*[12] (Pierre Gassendi) 的来往书信, 其中没有包括一些有关 "数" 的重要信件, 这显然是因为它们的收信人没有把它们交给塞缪尔的缘故; 因此它们至今仍不为我们所知.

现在有了由 P.Tannery 和 Ch. Henry 出版了四卷本的费马的全部工作 (巴黎 1891—1912; 及 C.de Waard 1922 年出版的《补遗 (*Supplément*)》), 但还必须再添加上梅森的《通信》和前面提到的 J.E. 霍夫曼出版物里的一些段落; 除非有进一步的发现, 可以假定我们已经有了一部完整的费马文集 (*corpus*), 但它必定会出现的不完整之处总在吊着我们的胃口.

§2.2 二项式系数

在履行我们的写作计划中, 将仅仅考虑费马在 "数" 方面的工作; 我们不仅把他在有关几何和微积分方面的广泛著述搁置不顾, 而且也不讨论他在概率论方面的重要工作 (包含在与帕斯卡 *Fe*.II,288–312, 和与惠更斯 *Fe*.II,320–331 的

*[12] 1592—1655, 法国哲学家、天文学家、科学家和教士.

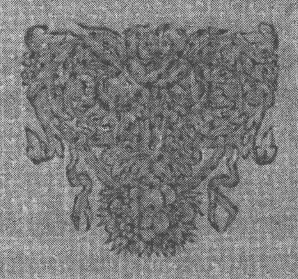
VARIA OPERA

MATHEMATICA

D. PETRI DE FERMAT,

SENATORIS TOLOSANI.

Accesserunt selectæ quædam ejusdem Epistolæ, vel ad ipsum à plerisque doctissimis viris Gallicè, Latinè, vel Italicè, de rebus ad Mathematicas disciplinas, aut Physicam pertinentibus scriptæ.



TOLOSÆ,

Apud JOANNEM PECH, Comitiorum Fuxensium Typographum, juxta Collegium PP. Societatis JESU.

M. DC. LXXIX.

《*Varia Opera Mathematica*》的扉页

通信中)，和对代数及消元理论方面的贡献，还有他对于罗梅[*13] (Adriaen Van Roomen) 的分圆方程的处理 (*Fe*.I,189–194).

或许二项式系数 (binomial coefficients) 更多地算是代数而非数论，即便是费马，在说到他对此的早期结果 (*Fe*.I,341,Obs.XLVI) 时，也评述道:" 很难找到有关数的更加漂亮、更具一般性的定理了". 所说的这个定理所涉及的数用现代的记号表示为

$$\binom{n+m-1}{m},$$

而费马和他的同代人则记述它们为 "三角形的" ($m=2$),"棱锥形的" ($m=3$), "三重三角形的 (*triangulotriangular*)" ($m=4$), 等等; 它们由下面的递归关系定义:

$$\binom{n+m}{m+1} = \binom{n+m-1}{m} + \binom{n-1+m}{m+1} = \sum_{\nu=1}^{n} \binom{\nu+m-1}{m}.$$

费马肯定注意到了在二项式公式中这些数所起的所用; 他或许已经知道了它，如果不是从斯蒂夫 (Stifel) [*14]那里 (他在不同的场合说过从来没有读过他的东西: *Fe*.II,188)，那么至少是从他研读韦达时知道的; 参看，譬如韦达的《*Ang.Sect*》,1615 年出版 (=*Op.Math*.287–304). 费马的定理只是公式

$$n \cdot \binom{n+m-1}{m-1} = m \cdot \binom{n+m-1}{m}.$$

当然我们无法确定费马在他的《丢番图》边白上所记笔记的日期; 但这一个肯定要早于他在 1636 年对罗伯瓦尔多少有点得意地提及 ("一个很好的命题 (*une tres-belle proposition*)") 的这同一结果 (*Fe*.II,84)，而后又对梅森提到它 ("*propositionem pulcherrimam*")(*Fe*.II,70; 对此信我们采用了 J.Itard, *Rev.Hist.Sc*. 2(1948),pp.95–98 所建议的日期:1638 年). 这个定理对他在 1654 年的关于概率论的工作有很大的好处; 所涉及的这后面的课题，帕斯卡也于同年独立地得到了，他相当奇怪 (因为他属于罗伯瓦尔这个圈子) 怎么会没有注意到费马的早先发现 (参看 *Fe*.II,308, 以及 *Fe*.II,70, 注 (1)). 在三十年代，费马主要用它来求出下面形式的和:

$$S_m(N) = \sum_{n=1}^{N} n^m,$$

或更一般的 $\sum_1^N (an+b)^m$. 显然 (参看 *Fe*.II,84) 他像上面那样把它写成

$$\binom{N+m}{m+1} = \sum_{n=1}^{N} \binom{n+m-1}{m},$$

[*13]1561—1615, 比利时数学家, 使用阿基米德的分圆法计算 π 到 16 位.

[*14]1487—1569, 德国数学家, 主要领域为算术和代数, 并独立于纳皮尔发明了对数.

并运用他的定理写出

$$\binom{n+m-1}{m} = \frac{1}{m!}n(n+1)\cdots(n+m-1)$$
$$= \frac{1}{m!}(n^m + A_1 n^{m-1} + \cdots + A_{m-1}n)$$

其中 $A_1, \cdots, A_{m-1}$ 为数值系数. 它给出了

$$S_m(N) + A_1 S_{m-1}(N) + \cdots + A_{m-1}S_1(N) = \frac{1}{m+1}N(N+1)\cdots(N+m),$$

由此, 对 m 可归纳地得到和 $S_m(N)$ 的公式. 当注意到 (*Fe*.II,68,84) 阿基米德已经知道了 $m=2$ 的情形, 巴歇也知道了 $m=3$ 的情形时, 费马则将 $m=4$ 作为一个样本, 并补充说明一般情形可用同样的方法处理. 同样的方式又被雅格布·伯努利 (Jacob Bernoulli) 再次发现 (在他死后 1713 年出版的《*Ars Conjectandi*》中), 使得他给出了 “伯努利数 (Bernoulli numbers)”和 “伯努利多项式” 的定义, 它们对于数论的重要性一直到后来欧拉的手中才显现出来. 至于费马, 在 1636 年向罗伯瓦尔叙述了上面的结果后, 他仅仅补充说 (*Fe*.II,35) 他已将它们应用于他对积分 $\int x^m dx$ 的计算 (还不如用他的话说, 计算 “抛物线” $y = x^m$ 的面积; 参看 *Fe*.II,73,94,95), 他在这里刻意地模仿了阿基米德在 $m=2$ 时用过的一种方法 (还可参看 *Fe*.II,83–84, 及 *Fe*.I,342,Obs.XLVIII).

§2.3 证明与“归纳”的相较

在将他的关于二项式系数定理告知罗伯瓦尔和梅森时, 费马没有说到他的证明. 另一方面, 在他的《丢番图》的边白上对此陈述以如下的话结束:“ *demonstrationem margini inserere nec vacat,nec licet*” (“我既无时间也无足够的地方在此边白上写下这个证明”), 这与他对方程 $X^n + Y^n = Z^n$ 的众所周知的陈述之后所写下的话 (“ 边白太窄而写不下证明” “*hanc marginis exiguitas non caperet*”) 十分相似. 在此顺带引起关注的这种巧合使得在费马更早所说的后面的那句话显得不可全信. 不管怎样, 对于费马对二项式系数定理的证明不会有多少怀疑; 如果如他所说, 他给出了这样的一个证明, 那么它只可能是一个用归纳法的证明. 当然它是帕斯卡在他的《算术三角形 (*Triangle Arithmétique*)》中以学究式的清晰所阐述的那个归纳证明, 它也是伯努利也在他的《猜度术 (*Ars Conjectandi*)》所同样做过的. 费马自己至少在他的一篇几何论文 “阿波罗尼奥斯 (*Apollonius*)” 中清晰地作出过一个归纳法的证明 (Lib.I, 命题 VII;*Fe*.I,26–27), 它大体是在 1630 年之前写的, 其完成则不会超过 1636 年 (*Fe*.II,100).

在那些年月, 甚至以后很久, “归纳” 这个词是以一种完全不同的意义在使用; 它表示的只是现在所理解的 “猜想” 的意思. “以归纳” 证明一个依赖于整数

n 的陈述 $P(n)$, 仅仅意味着对它的开始几个 (有时是非常少的几个) n 值进行证明. 当然也会出现所使用的方法的那种情况: 譬如, 从 $P(3)$ 导出对 $P(4)$ 证明的方式明显地表明以同样的推理可用作从 $P(n-1)$ 推导出 $P(n)$. 这种情况在欧几里得那里并不罕见 (譬如, 顺手便可在 *Eucl.*I,45,VII,14,VIII,6, 举出一些例子); 这时, 数学家有权将这样的证明视为是终结性的, 虽然它并没有用现在使用的那些约定的术语. 对于这样的证明, 习惯地使用 "完全的"(或 "数学的") 归纳法这种术语[4], 而 "不完全" 归纳则意味上面所描述的那种试探性的推理.

"不完全" 这种类型的归纳法被沃利斯十分系统地用于他 1656 年的《无穷的算术 (*Arithmetica Infinitorum*)》中, 并应用到多种多样的问题, 其中包括二项式系数的理论; 他的结果最终导致了牛顿的二项式级数, 以及下个世纪的欧拉的欧拉积分理论和 Γ 函数. 但是在这里我们必须强调指出费马对于沃利斯使用的 "归纳法" 的批评:

"如果某个命题的证明隐藏得很深, 并且在找出这个证明前如果希望首先说服自己多少相信它是正确的, 那么他可以使用这个方法; 但人们只应该对它抱有有限的信心, 并真正谨慎地使用. 的确, 人们可以提出如此一个问题, 并以这样的方式去寻求对它的证明, 它或许在许多特殊情形时成立, 但尽管如此还是错的, 并不普遍成立, 因此人们必须极其慎重地使用它; 无疑如果谨慎使用的话它仍是具有价值的, 但不能如沃利斯想要做的那样, 将其用来构建某个科学分支的基础, 因为对于这个目的, 没有证明是行不通的" ["*On se pourroit servir de cette méthode, si la démonstration de ce qui est proposé étoit bien cachée et qu'auparavant de s'engager à la chercher on se voulut assurer à peu près de la vérité; mais il ne s'y faut fier que de bonne sorte et on doit y apporter les précautions nécessaires. Car on pourroit proposer telle chose et prendre telle règle pour la trouver qu'elle seroit bonne à plusieurs particuliers et néanmoins seroit fausse en effet et non universelle. De sorte qu'il faut être fort circonspect pour s'en servir, quoiqu'en y apportant la diligence requise, elle puisse être fort utile, mais non pas pour prendre pour fondement de quelque science ce qu'on en aura déduit, comme fait le sieur Wallis; car pour cela on ne se doit contenter de rien moins que d'une démonstration...*":*Fe.*II,351–352].

可以预料, 这惹得沃利斯颇不高兴, 并在给迪格比的一封信 (*Comm.Epist.*, letter XVI= *Wal.*II,782–783) 中傲慢地拒绝了这个告诫. 因为他的结果大体上为后来的进展所证实, 回过头来看, 费马的批评可能给我们一种过于苛刻的深刻印象, 尽管他也以对沃利斯的高度赞扬淡化了这个批评 (也可参看 *Fe.*II,337,343).

[4]在法语中用 "递归 (récurrence)"(指 "完全的" 归纳) 避免了 "归纳 (induction)" 的双重含义 (有 "感应" 和 "归纳" 两个意思 —— 译注) 带来的歧义.

但我们在这里所关切的是费马对于证明的成熟观点. 类似地, 在 1662 年写给克莱塞里尔*15 (Claude Clerselier) 的信中, 他还写道 “证明的精髓是使你不得不相信” (“*la qualityé essentielle d'une démonstration est de forcer à croire*”:*Fe*.II,483). 当然, 毫无疑问他是个容易犯错误的人; 或许由于他的极少写下全部证明的要命习惯, 以及几乎不曾保存他与朋友们通信的复件, 他比别人更容易出错. 但是考虑到上面所引述的他的话, 那么当费马声称他对某个陈述有证明时, 我们不得不对此认真看待.

§2.4 完全数与费马定理

人们对于数的喜爱或许要比数论更早; 或者正是这种喜爱催助了数论的诞生; 它们一直是忠实伴侣, 尽管有时由于盲目崇拜也并非完全无可指责 (参看第一章 §3). 如前面所说到的 (第一章 §9), 印度人对于大的数的喜爱可能给了他们处理佩尔方程的一种契机. 在转向丢番图之前, 巴歇也一直是个数的热爱者 (参看第一章 §12).

或许在费马的同时代的人中没有能够称得上数论学家的人; 但是许多人却都是数的热爱者. 其中一位便是梅森, 他喜欢 “完全” 数与 “亲和” 数; 同样如此的还有比费马年纪大的 P.Bruslart de Saint Martin 和 A. Jumeau de Sainte Croix, 以及比费马年轻几年的弗莱尼柯 (参看第一章脚注 *15), 后来他成了在 1666 年由柯尔贝尔*16 (Colbert) 建立的首个法国科学院的院士. 弗莱尼柯曾被费马赞扬道:“未借助于代数, 这位天才如此深入地洞察了数的知识”, 这或许并没有丝毫嘲讽之意 (*Fe*.II,187).

在他事业的早期, 即在波尔多的时期 (参看 *Fe*.II,196), 费马就被 “幻方 (magic squares)” 吸引; 这是些满足一些线性条件的正整数的方阵. 斯蒂夫, 卡尔达诺, 巴歇都曾提到过这个课题. 1640 年, 通过梅森, 费马和弗莱尼柯发现了他们对此的共同兴趣; 这成了他们之间通信往来的开端 (参看 *Fe*.II,182–197), 在多少有点不太顺利的开头 (*Fe*.II,182–185) 之后, 很快便转到更加实质性的话题, 尽管有一些偶然的摩擦, 通信还是断断续续地持续了二十来年.

尽管费马公开声称他热衷于幻方 (*Fe*.II,194), 并且卢卡斯*17 (E. Lucas) 颇具吸引力的提示 (*Fe*.IV,190) 说它可以引向四平方和基本公式的发现 (参看下文的 §14 及第三章 §11), 但我们仍难于认真对待它. 在那个时候更加受到数迷们欢迎的课题则由于费马的参与而远较其他更富于成果; 它就是从欧几里得关于 “完

*15 1614—1684, 法国编辑, 编撰了笛卡儿的著作和来往书信.

*16 1619—1683, 法国路易十四时的财政大臣、海军国务大臣, 致力于建立法国的经济霸权.

*17 1842—1891, 法国数学家, 以研究斐波那契数而知名. 他设计了一个素数的检测方法, 后经改进为对梅森数的 Lucas—Lehmer 检测法.

全数”定理发展出来的课题，并且在费马那个年代，它总是一成不变地被冠以一个十分不恰当的名字:“可整除部分 (aliquot parts)”. 不知何故，这个不知出自何处的术语 “*aliquot part*” 表示一个整数 n 的任一个因子，包括 1 但不包括 n，而复数格的 “*aliquot parts*” 则表示了这些因子的和 $s(n)$. 那么，“完全” 数是指那些满足 $s(n) = n$ 的数，“亲和” 数则是指一对数 n, m，使得 $s(n) = m$, $s(m) = n$. 除此以外，梅森和其他一些人开始寻找 “次倍 (submultiple)”*18 数，即 $s(n) = a \cdot n$ 的解，其中 a 为 2,3 或其他小的整数. 甚至在 1638 年左右，笛卡儿也被吸引来研究这种数了；并且以他一贯的傲慢，不久便成了这场竞赛的自封冠军，在此同时，他向弗莱尼柯 (这个称号的竞争对手) 保证说，这只不过是在他听到这件事的不到一年时间做到的. 这是笛卡儿哲学的一个基本原则，即一个靠*真正*自我修养的力量和*真正*运用推理能力的人，能够在他自身思想里构建成一个了解物质和非物质世界的一切事物的完整体系. 这里着重强调的是*真正*这个字眼，当然它原来是指笛卡儿，也只有他，才会有这样的业绩，因此别人可以向他好好地学习，而他则从别人那里学不到也无需学什么东西. 譬如，他坚决否认他的代数中有任何知识来自韦达，不管是直接还是间接的；但是不太可能有人出来说，没有什么办法来检验它们的真实程度吧.

实际上，在那时的费马、梅森、弗莱尼柯以及笛卡儿之间的交换信件中所出现的话是说，要想得到所有的 “完全”、“亲和” 和 “次倍” 数需要的不仅仅是一点点的聪明才智. 费马早在 1636 年之前就开始考虑这些问题了 (*Fe.*II,20)；在 1636 年他曾断言，如果他想要得到解决所有这些问题的一般的方法是非常困难的，并且告诉罗伯瓦尔说，他计划写一篇关于这个题目的小文章 (*Fe.*II,93)；1643 年，他还得意地说到关于 *aliquot parts* 的 “卓越发现”，但是他对它们的兴趣似乎正在消退 (*Fe.*II,255)；那时丢番图问题和平方和问题已经占据了显著的位置.

要想了解这个问题对于与费马同代的一些人的困难程度，我们一定要记住，迟至 1640 年 (*Fe.*IV,69)，梅森还在问 Saint-Martin，在不用一个个去数的情形下，如何求出 49000 的因子的个数以及它们的和；欧几里得，甚至还有环绕在柏拉图周围的数学家们 (参看第一章 §2)，或许已经发现了这是一个自然的问题. 一个好的代数记号对于这样一些问题当然有极大的帮助；用笛卡儿和费马所使用的这种记号，几乎可平凡地证明，当 p 为素数时，对任意的 n 则有 $s(p^n) = (p^n-1)/(p-1)$ (从实质上说，这个结果已包含在 *Eucl.*IX,35 中). 为方便起见，如果记 $S(n)$ 为包括 n 在内的 n 的因子的和，即 $S(n) = s(n) + n$，那么当 m, n 互素时，同样容易证明 $S(mn) = S(m)S(n)$. 上面的这两个结果都出现在欧几里得关于完全数定理的证明的最后部分，他的这个定理是说，如果数 $2^{n-1}(2^n - 1)$ 的第二

*18这里所用的该字的中文不同于通常翻译的 “约数”,“因数”.

个因子是素数, 则该数为完全数[5]. 同样地, 可以证明笛卡儿在 1683 年交给梅森的关于亲和数 (amicable numbers)的一个规律: 对于数 $2^{n+1}(18\times 2^{2n}-1)$ 和 $2^{n+1}(3\times 2^n-1)(6\times 2^n-1)$, 如果第一个数的第二个因子, 和第二个数的第二个和第三个因子均为素数, 则这两个数为亲和的 (*Desc.*II,93–94); 费马对此规律也肯定知道, 事实上还要早得多 (*Fe.*IV,185). 在当时所构造的那些数中我们只举出另一个例子: 这是一个满足 $s(n)=5n$ 的数, 它可分解因子为

$$\begin{aligned} n =& 2^{36}\times 3^8\times 5^5\times 7^7\times 11\times 13^2\times 19\times 31^2\times 43\\ &\times 61\times 83\times 223\times 331\times 379\times 601\times 757\\ &\times 1201\times 7019\times 112303\times 898423\times 616318177. \end{aligned}$$

这是 1643 年由弗莱尼柯通过梅森向费马展示的 (*Fe.*II,255); 从费马的反应来看, 似乎他一定早已知道了. 容易看出, 构造这样的数的整个关键点在于确定某些大数, 特别是形如 2^n-1, 3^n-1 这样的一些数是否是素数, 如果不是, 则将其分解成它们的素因子. 譬如, 在 1640 年, 弗莱尼柯还是通过梅森向费马提出寻找在 10^{20} 与 10^{22} 之间的一个完全数 (*Fe.*II,185); 这个问题隐含着与 "欧几里得" 完全数 —— 即形如 $2^{n-1}(2^n-1)$ 的数 —— 的一些关联, 因为在那时除这种形式外不知道有其他的这种数 (现在也确实不知). 不等式

$$10^{20}<2^{n-1}(2^n-1)<10^{22}$$

给出 $34\le n\le 37$, 并且除非 n 为素数, 否则 2^n-1 不可能为素数, 这是因为对任意的 a 和 b, 2^a-1 除尽 $2^{ab}-1$. 因此弗莱尼柯问题的关键点真正在于找出 $2^{37}-1$ 是不是一个素数. 费马很快回答: 它不是, 从而在 10^{20} 与 10^{22} 之间没有完全数 (或者至少是没有 "欧几里得" 完全数)(*Fe.*II,194); 幸亏由于他的自尊心, 及时地发觉了他计算中的一个数值误差, 这险些让他落进了弗莱尼柯为他精心设计的一个陷阱中 (*Fe.*II,199). 他发现的是分解

$$2^{37}-1=137438953471=223\times 616318177.$$

同时, 如果我们还留意到下面的素因子分解:

$$\begin{aligned} &616318177+1=2\times 7^3\times 898423,\\ &898423+1=2^3\times 112303,\\ &112303+1=2^4\times 7019,\\ &7^8-1=2^6\times 3\times 5^2\times 1201,\\ &3^9-1=2\times 13\times 757, \end{aligned}$$

[5]欧拉证明了这些是所有的偶完全数; 其证明不难, 或可作为习题推荐给读者.

那么, 便有了用于检验上面提到的弗莱尼柯的 "次倍" 数所需要的一切.

让我们更加感兴趣的是费马为分解 $2^{37}-1$ 所采用的方法. 根据他在 1640 年 6 月左右告诉梅森的 (*Fe*.II,198), 他的方法根据了下面的三个命题:

(I) 如果 n 不是素数, 则 2^n-1 也不是素数.

(II) 如果 n 是素数, 则 2^n-2 是 $2n$ 的倍数.

(III) 如果 n 是素数, 并且 p 是 2^n-1 的一个素因子, 则 $p-1$ 是 n 的一个倍数.

正如前面一提到的那样, (I) 是平凡的, 因为它是恒等式

$$x^b-1=(x-1)(x^{b-1}+x^{b-2}+\cdots+1)$$

中 $x=2^a$ 的特殊情形. 费马把此当作一个发现提了出来恰恰说明在那时他的代数知识是何等肤浅. 至于 (II) 与 (III), 它们自然是现在称之为 "费马定理" 的典型情形. 对于它的一般性阐述, 我们不得不拿出他在 1640 年 10 月 18 日给弗莱尼柯的信, 在那里他把它们称为 " aliquot parts 的基本命题 (*la proposition fondamentale des parties aliquotes*)" 并作了如下的叙述 (*Fe*.II,209):

"已知任一素数 p, 及任意几何级数 $1,a,a^2$, 等等, p 必定除尽某个数 a^n-1, 其中 n 除尽 $p-1$; 如果 N 是具此性质的最小数的倍数, 则 p 也除尽 a^N-1."

实际上用 "归纳法", 即实验方法, 不难发现这个断言, 譬如在 $a=2$ 这个对完全数具有决定性的情形. 倘若弗莱尼柯知道了它, 我们则可设想他是按此方式进行的: 实际情况也大体如此吧; 在 1676 年到 1680 年间, 莱布尼茨也是这样做的[6]; 在 1731 年及以后的年月里, 欧拉也这样做了: 在他关于数论的最早的文章中写道: " *tentando comprobari potest*", 即 "它的真实性可有实验证实" (*Eu*.I-2,1 于 E26 中, 1732; 参看第三章§4). 我们几乎不怀疑费马也是以同样的方式得到了它的; 但是在 1640 年他已说过它有一个证明: 他写道 " 如果弗莱尼柯不嫌太长的话, 会将它交给他". 这会是个什么样的证明呢?

对于费马定理有两个经典的阐述, 从而有两个相应的证明. 像费马在给梅森的信中对 $a=2$ 所写的那样, 将其记为 $a^p\equiv a \pmod p$, 可以以加法的方式对 $a=2$ 写成

$$2^p=(1+1)^p=1+\binom{p}{1}+\binom{p}{2}+\cdots+\binom{p}{p-1}+1$$

并看出在右端的二项式系数都是 p 的倍数; 这确实包含在费马关于二项式系数所证明的东西之中, 它不迟于 1636 年 (参看前面的 §2). 同样的结果或者用 "数

[6]在莱布尼茨的未发表的在数论方面的偶然之作上, 参看 D.Mahnke 的极好文章: *Bibl.Math.*(3) 13 (1912–13),26–61.

学归纳法” 拓展到 $a>2$: 像欧拉在 1742 年所做的那样, 记

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1,$$

或者像莱布尼茨所做的那样, 使用 “多项式公式”

$$(1+1+\cdots+1)^p = 1+1\cdots+1+\sum_{q+r+\cdots+s=p}\frac{p!}{q!r!\cdots s!}$$

(参看 D. Mahnke, 同上, p.49).

另一方面, 如果将此定理按费马在他给弗莱尼柯的信中那样写出, 它则是以下事实的特殊情形: 一个群的阶是其任意子群阶的倍数. 我们首先要看到, 如果以 p 除以几何级数 $1, a, a^2, \cdots$ 的每一项, 其中 a 与 p 互素, 那么它们的余数必定会重复, 于是对于某个 $r \geq 0$ 和某个 $n > 0$ 我们便有 $a^{n+r} \equiv a^r$, 即 $a^r(a^n-1) \equiv 0 \pmod p$; 它给出了 $a^n \equiv 1 \pmod p$; 取 n 为使其成立的最小的数; 于是我们可以把这 $p-1$ 个与 p 互素的 $\bmod p$ 的同余类排列成形如 $\{b, ba, \cdots, ba^{n-1}\}$ 这样的一些集合, 其中每一个集合由 n 个元构成; 容易看出这些集合互不相交, 故 n 必除尽 $p-1$. 这是欧拉在 1750 年左右得到的乘法性证明, 他说到这个方法时表示这是一个比较好的方法, 因为它可以被推广到 $a^{\phi(m)} \equiv 1 \pmod m$, 其中 m 为任意整数 (参看第三章§6). 鉴于费马将他的定理的阐述方式从 (II) 改变为 (III), 而后改变成了他对弗莱尼柯的那个陈述, 我们可以推测他的最后证明可能就是第二个.

至于如何应用它, 费马解释得十分清楚. 以上面的 $2^{37}-1$ 为例. 如果它有一个素因子 p, 那么 37 必定除尽 $p-1$; 由于 p 为奇数, 它必定以 $74n+1$ 的形式出现; 在淘汰了第一个可能的数 149 后, 下一个 223 则是成功的 (*Fe.*II,199).

费马的探询并没有停留在那里. 在将形如 a^n-1 分解因子时, 我们立刻注意到, 对于 $n=2m$ 必须要对数 a^m+1 进行分解; 于是费马问道, 对于任意 a 及任意素数 p 是否总有 m 使得 p 除尽 a^m+1. 当然, 答案是否定的, 而费马对于出现这种情形给出了一个判别准则: 其充要条件是 p 除尽 a^n-1 的最小 n 是个偶数; 于是存在 m 使得 p 除尽 a^m+1, 且最小的这种 m 为 $n/2$ (*Fe.*II,209–210).

对于 $a=2$, 费马又产生了另一个问题, 从 “aliquot parts” 的角度看也是一个重要的问题: 什么时候 2^m+1 是个素数? 如果 m 具有一个奇数因子 $d>1$, 则不是这种情形, 因为如果 $m=ed$, 则令 $N=2^e$ 时便立刻知道 $N+1$ 除尽 $2^m+1=N^d+1$. 那么剩下来的情形便是 $m=2^r$; 于是对于 $r=0,1,2,3,4$, 2^m+1 确实是素数. 在 1640 年给弗莱尼柯写信时, 费马已将这种数算到了 $r=6$:

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617,$$

并猜测它们全是素数. 很难相信他不曾将他用于分解 $2^{37}-1$ 的方法用于, 至少是第六个数 $2^{32}+1$ 的分解上; 这表明 $2^{32}+1$ 的素因子具有形式 $64n+1$, 可能的数有 $193, 257, 449, 577, 641$, 等等; 641 除尽 $2^{32}+1$; 事实上, 这正是差不多一百年后欧拉如何附带地重新发现那种费马定理的情形 (参看第三章§4). 更令人惊讶的是, 对 $2^{37}-1$ 进行过分解的弗莱尼柯, 也没有立刻指出这个错误, 尽管他很不情愿这样做 (从他们之间通信的一般语调来判断; 参看 *Fe.*II,185); 相反地, 弗莱尼柯与他保持了一致 (*Fe.*II,208). 费马直到死都坚持了这个猜想, 并且通常还补充说他对此还没有完全的证明 (参看 *Fe.*II,309–310, 在那里他提到, 这对于 "aliquot parts" 是重要的; 也可参看 *Fe.*II,405,434). 我们可以想象, 当他第一次构思了这个猜想时, 由于激情而不能控制自己从而犯了一个计数的错误, 之后也再没有去检查他的计算. 至于 $2^{64}+1$, 它有素因子 274177, 这无疑超过了费马的计算能力, 甚至也超越了弗莱尼柯的, 尽管他们两个中后者是个更顽强的计算者. 即便验证 616318177 是个素数也必定已痛苦地考验了费马的耐心, 当然, 如果他真的曾奋力做过这个计算的话.

§2.5 最初的探索

从 1636 年到 1640 年间, 费马把他的注意力不断地转向了两类问题: 一个是丢番图问题, 另一个则是平方和问题.

当然后一类问题也是由丢番图提出的, 至少也是由巴歇在对丢番图的评注时提出的 (参看第一章 §11). 我们所看到的是出现在 1636 年费马与梅森通信的初期. 出现在这些信件中的第一批问题的一个相当于是问, 一个等于两个 (分别地, 三个) 有理数平方和的整数是否也是两个 (分别地, 三个) 整数的平方和; 丢番图似乎将此认作是理所当然的, 巴歇在他的评注中亦然 (参看, 譬如在他的评著 *Dionph.* V,9=V,12_b 以及 *Dioph.*V,11=V,14_b 中). 费马给梅森的 1636 年 7 月 15 日的信 (*Fe.*II,29–30) 意味着这是个他认为他已经证明了它的日子, 但在 1636 年 9 月 2 日他却仅仅说他正在做这件事 ("*c'est à quoy je travaille*"; *Fe.*II,58). 对此的一个初等证明在 1912 年由 L.Aubry 发表 (参看第三章的附录 II); 这是一个费马能够明白的证明. 当然我们无须去探询他是否已经找到了对此证明; 如果他找到了, 他有的是机会去向他的通信人提及的; 然而这种事再也没有出现在他的信件中.

显然, 在那几年里, 对于涉及 "数" 方面来说费马还只是个生手. 在 1636 年 9 月 16 日他用欧几里得的第 10 书的术语向罗伯瓦尔提出了一个问题; 它相当于说要证明

$$x^2+y^2=2(x+y)z+z^2$$

在有理数中没有非平凡解. 几天之后的 1636 年 9 月 22 日, 他找到了一个它的证明, 但是却做得十分辛苦 (“*elle m'a donné grandissime peine*”: *Fe*.II,74). 他的证明, 也是罗伯瓦尔同时找到的那个证明是: 令 $t = z + x + y$, 并将该方程改写成

$$2x^2 + 2xy + 2y^2 = t^2,$$

然后看出, 如果取 x, y, t 为没有公因子的整数, 那么 t 必为偶数, 因此 x 和 y 不会全为偶数, 从而 $x^2 + xy + y^2$ 必为奇数. 换句话说, 该方程没有非平凡解, 甚至作为 mod 4 的同余方程也没有. 我们也可以观察到, 原方程可以写成

$$3z^2 = (x - z)^2 + (y - z)^2,$$

从而此方程表明不是两个整数平方和的 3 也不是两个有理数的平方和. 这是他在此前不久向梅森提及的一个问题的特殊情形. 它也可以由考虑同余式 $3z^2 \equiv u^2 + v^2 \pmod 3$ 给出同样完美的回答.

实际上, 借助于 “哈塞原理” (“Hasse's principle”) (参看第四章附录 I) 得知, 如果 F 是任一具整系数的二次不定式, 并且如果 $F(x) = 0$ 没有非平凡整数 (或等价地, 有理数) 解, 则存在一个模 m 使得同余式 $F(x) \equiv 0 \pmod m$ 也没有非平凡解. 换句话说, 在单个的二次齐次方程情形, 这种类型的不可解性总可以以一个同余式的论证来证实; 特别它可应用到将一个数表示为平方和的问题上. 那么, 在费马作为数论学家的初期, 他以此类问题作为起步便不足为奇了. 他还没有将同余式的论证法看成本质上平凡的方法, 只不过说明在那时他缺少历练; 这必定曾经给他造成过某些尴尬. 1638 年, 他在写信给梅森 (*Fe*.II,66) 时颇为得意地宣布, 形如 $8n - 1$ 的整数都不是少于四个平方数的和, 不仅是整数的甚至分式的平方和也如此; 除此之外, 他显然在较早的信中已陈述过了关于形如 $4n - 1$ 的数与两个平方和的相似事实. 梅森按其一贯的做法, 将它转交给笛卡儿, 而笛卡儿那时认为他有理由相信费马冒犯了他. 实际上, 凡是涉及整数的平方, 巴歇都已经按照模 8 同余或模 4 同余给出了证明 (索引同上). 笛卡儿以傲慢的姿态指出容易将其推广到分数; 装着对此平凡小事不屑一顾的样子, 他甚至把它交给一个据说是没有受过正规学校教育的年轻人去做, 实际上这个人是他以前的学生简 · 热罗 (Jean Gillot) (*Desc*.II,179,195; 参看同上的 II,91–93, 以及 F.Rabelais 的《*Pantagruel*》,Livre II,Chap.XVIII).

令人吃惊的是，尽管费马在 1638 年给梅森的这封信中关于形如 $8n - 1$ 的陈述在不知情的情形下使自己遭受到了笛卡儿的嘲讽, 但紧随此之后则是那个著名的陈述, 即任一个整数是 “ 三个三角数、四个平方数、五个五角数, 等等之和”. 这与他在其《 丢番图 》书边白上记下的是一样的 (*Fe*.I,305, Obs.XVIII), 或许它们是在同一个时间写下的吧; 在 1654 年他又把它写给了帕斯卡 (*Fe*.II,313),

1658 年还写给了迪格比 (*Fe*.II,404). 在 1638 年的这封信中还向 Sainte-Croix 挑战以找出两个立方数使其和仍为立方数, 或者两个四次幂其和仍为四次幂, 这意味着他已经知道了或者已察觉到没有这样的数. 我们永远不会弄明白费马在何时, 或者是否证明了这些结果. 但在 1638 年他还是一个数论的新手的时候, 他的天赋已经开始闪闪发光了.

§2.6　对二次剩余的初次尝试

我们先把平方和问题放在一边, 转而讨论自欧拉以来我们对二次剩余理论知道了些什么.

我们已经看到, 费马定理是从想要求出一个素数 p 何时能够除尽数 a^n-1 的问题中产生的; 与此问题相伴的是求出何时 p 除尽 a^n+1 的问题, 这在他与弗莱尼柯的 1640 年和 1641 年的通信中反复出现过 (*Fe*.II,209–210, 220,226,232). 用现代的术语表达, 我们说 $n_p(a)$ 是 a 模 p 的阶是指一个最小的数 $n>0$, 使得 p 除尽 a^n-1. 由费马判别法 (参看前面的 §4), p 除尽某个数 a^m+1 的充要条件是 $n_p(a)$ 为偶数. 另一方面, 从欧拉以来便已知道, a 是一个模 p 二次剩余的充要条件是 $(p-1)/n_p(a)$ 为偶数; 由二次互反律, 满足该性质的素数 p 是那些出现在形如 $4ax+b$ 的某个算术级数中的数, 这是欧拉所发现的, 而 "由归纳法" 则更容易得到它 (参看第三章§8). 如果仅仅考虑形如 $4n-1$ 的素数, 那么当 $(p-1)/n_p(a)$ 为奇数时 $n_p(a)$ 则为偶数, 反之亦然; 因此, 对这样的素数, 有一个基于二次剩余的简单判别法, 以判断 p 是否具有费马所要求的性质; 对于其他的数, 则没有这类的判别法. 然而有点奇怪, 费马竟认为这是个非常困难的问题 (*Fe*.II,210)! 从它的特别之处来看, 或许是因为当他尽力以实验的方法进行探索时, 他很快就犯了平凡的数值错误, 从而使他打消了继续尝试的念头. 在他 1641 年给梅森的信中以及打算写给弗莱尼柯的文字中 (*Fe*.II,220–221) 他断言: (A) 形如 $12n\pm1$ 的素数不能除尽形如 3^m+1 的整数; (B) 每个形如 $12n\pm5$ 的素数除尽某个 3^m+1; (C) 素数 $10n\pm1$ 不能除尽 5^m+1; (D) 每个素数 $10n\pm3$ 除尽某个 5^m+1; 作为例子, 对 (A) 他列举了 11, 13, 23, 37, 对 (B) 举出了 5, 17, 19, 对 (C) 为 11, 19, 而对 (D) 则列举了 7, 13, 17. 他甚至许诺 " 对另外情况" 有素数除尽 a^m+1 的一般法则, 其中 a 任意. 实际上, 类型 (A) 的 (分别地, 类型 (B) 的) 素数使 3 为二次剩余 (分别地, 非二次剩余), 而类型 (C) 的 (分别地, 类型 (D) 的) 是使 5 为二次剩余 (分别地, 非二次剩余) 的素数. 费马的断言对于形如 $4n-1$ 的素数是对的, 但对其他的则未必如此; 事实上, 37 是 (A) 的一个反例, 这是因为它除尽 3^9+1; 另外, 41 除尽 $5^{10}+1$ 给出了 (C) 的一个反例. 因此费马错过了猜测到二次互反律的机会; 作为事后诸葛亮, 我们知道是他

问了一个错误的问题.

无疑, 处理 -1 的二次特征标要更容易些, 尽管如此, 在那时必定仍被看成是一个重要发现. 费马在 1640 年写给罗伯瓦尔的信中断言 (*Fe.* II,204), 如果 a 和 b 互素, 则 a^2+b^2 的素因子都不具有 $4n-1$ 的形式. 换一种说法, 如果一个整数具有形如 $4n-1$ 的素因子, 并且没有平方因子, 则它不能被表成两个平方数的和 ("甚至不是分数的平方和"). 稍后写给弗莱尼柯 (*Fe.*II,210) 时, 他把它拆开为一个语义模糊的陈述, 而它其实就是寄给罗伯瓦尔的那个定理的一个直接推论. 不管是弗莱尼柯还是费马, 在那个时期都不愿意把他们的最好结果透漏给对方. 当在此同一封信里, 费马告诉弗莱尼柯说, 一个形如 x^2+2 的素数不能除尽数 a^2-2 时 (*Fe.*II,211), 人们不禁要怀疑是否他在测试弗莱尼柯的知识水平, 或者是要故意误导他; 事实上, 这样的一个素数显然具有 $4n-1$ 的形式, 并除尽 $a^2+x^2=(a^2-2)+(x^2+2)$.

至于费马的证明, 必定与欧拉在 1742 年所发现的证明相同 (参看第三章§5b). 假设 $p=4n-1$ 是个素数, 除尽 a^2+b^2, 且 a, b 互素; 那么 a 和 b 都与 p 互素. 为简便计用现代的记号表示, 我们有 $a^2\equiv -b^2 \pmod p$; 令 $m=2n-1, p-1=2m$, 则有 $a^{2m}\equiv -b^{2m} \pmod p$. 但由费马定理, $a^{2m}\equiv b^{2m}\equiv 1 \pmod p$; 矛盾.

§2.7　两个平方数和的素因子

我们对于模 p 同余类构成域, 即所谓的素域 $\mathbb{F}_p$, 这个事实已习以为常了, 同样还有它所蕴涵的所有代数性质也是如此, 从而我们觉得没有必要再对它进行进一步的分析. 实际上巴歇对于方程 $ax-my=1$ 的解 (参看第一章 §4) 表明了每个与 m 互素的整数 a 都有一个模 m 逆; 对于素数 m 这便表明了 $\mathbb{F}_m$ 是个域. 同样的这个事实也可看作费马定理的一个推论, 这是因为同余式 $a^n\equiv 1 \pmod p$ 意味着 a 以 a^{n-1} 为模 p 逆. 由此, 譬如, 我们可立刻推导出: 当 a 和 b 与 p 互素, 那么, 如果 p 除尽 a^2+b^2, 则 -1 是一个模 p 的二次剩余; 事实上, 如果 a' 是 a 的模 p 逆, 那么同余式 $x^2\equiv -1 \pmod p$ 有解 $x=a'b$. 因此费马写给罗伯瓦尔的那个结果以现代术语表示等同于确定了 -1 模 $4n-1$ 形素数的二次剩余特征标. 费马必定在某个时间已经留意到此; 他以后的一些结果不可能再加以别的什么解释了 (参看下文的 §12).

$p=4n+1$ 的情形必定给他带来了更多的麻烦, 这正如同它带给了欧拉更多的麻烦, 也给那些力图解开费马的数论秘密的历史工作者们带来更多的麻烦一样. 实际上, 不仅每个形如 $p=4n+1$ 的素数除尽某个和数 a^2+b^2, 而且每个这样的素数本身也可以以唯一一种方式写成 a^2+b^2. 第一个发表了对这些事实证明的人是欧拉; 而它们早在 1640 年已被费马陈述过了 (*Fe.*II,213; 参看 *Fe.*I,314,

Obs.XXVI, 以及 *Fe.*I,293, Obs.VII). 在所有已知的证明中, 人们总不得不从证明其第一部分着手, 即证明 -1 是一个 $p=4n+1$ 的二次剩余, 这必定也是费马当时的状况 (参看 *Fe.*II,432, 以及下文的 §8). 如果再考虑到欧拉 (*Corr.*I,494; 参看第三章§VI) 我们便会明白费马可能是如下进行证明的.

取一个素数 $p=4n+1$, 并且对与 p 互素的 x, y 令 $a=x^n$, $b=y^n$. 我们有

$$(a^2+b^2)(a^2-b^2)=x^{4n}-y^{4n}.$$

由费马定理知这个数是 p 的一个倍数, 故 p 或除尽 $a^2-b^2=x^{2n}-y^{2n}$ 或除尽 a^2+b^2. 那么, 如果 p 不除尽所有形如 a^2+b^2 的数, 其中 a, b 与 p 互素, 它则必定除尽所有的数 $x^{2n}-y^{2n}$; $y=1$ 给出了 $x^{2n}\equiv 1 \pmod p$, 其中 $1\le x\le p-1$.

如我们现在所知道的那样, 一个 d 次的同余式在 $\mathbb{F}_p$ 中解的个数不会超过 d 个; 特别地, 同余式 $x^{2n}\equiv 1 \pmod p$ 不可能有 $p-1=4n$ 个解. 对我们来说, 这个简单的注解就足以把此搞定. 为了引用方便, 我们把所考虑的结果正式叙述成一个引理:

引理 1. *设 p 为素数; 于是不存在数 $m<p-1$ 使得对所有与 p 互素的整数 a, a^m-1 是 p 的倍数.*

或许基于一定数量的数值依据, 费马是否已将此视为理所当然的事了? 当然他知道一个 m 次方程 $f(x)=0$ 不可能有超过 m 个解; 譬如在 1636 年的笛卡儿的《几何学 (*Géométrie*)》中便有对此的证明 (*Desc.* VI,444–445), 我们在此想给出他的这个证明: 如果 $f(x)=0$ 具有根 $x_1,x_2,\cdots,x_n$, 人们便可以相继地以 $x-x_1,x-x_2,\cdots,x-x_n$ 去除 $f(x)$, 从而将次数降到 $m-n$; 这里所在的域被理解为实数域. 在 1772 年, 欧拉意识到这对域 $\mathbb{F}_p$ 同样有效 (参看第三章§6); 所涉及的证明步骤相当容易. 然而我们会把欧拉只是在他长期数学生涯后期才达到的, 具有一定程度抽象思维的东西归于费马吗? 很可能不会如此.

在 1749 年欧拉对此以不同的方式进行了处理 (引文同上); 作为莱布尼茨和伯努利的真正门徒, 欧拉使用了差分算子 D, 其定义为

$$(Df)(x)=f(x+1)-f(x);$$

由对 m 的归纳容易看出, 对任意的 m, $D^mf(x)$ 是 $f(x)$, $f(x+1),\cdots,f(x+m)$ 的整系数线性组合. 因此, 对某个 $m<p-1$ 如果对所有 $1\le a\le p-1$, p 除尽 a^m-1, 则它也必定除尽 $D^mf(1)$, 其中 $f(x)=x^m-1$; 但欧拉知道, 经由对 m 的简单归纳可看出 $D^mf=m!$; 因为 p 为素数而 $m<p-1$, 故这不可能是 p 的倍数.

对 -1 的二次特征标的另一个证明是拉格朗日在 1771 年给出的 (*Lag.*III,425–438), 它不仅依赖于引理 1, 而且也依赖于 “威尔逊定理 (Wilson's theorem)”, 即对任意素数 p 成立同余式 $(p-1)! \equiv -1 \pmod p$. 如果知道了或者假定了这个同余式, 则只要对 $p = 2m+1$ 写出

$$\begin{aligned}(p-1)! &= (1 \times 2 \times \cdots \times m) \cdot (p-1) \cdot (p-2) \cdot \cdots \cdot (p-m) \\ &\equiv (m!)(-1)^m m! \\ &\equiv (-1)^m (m!)^2 \pmod p\end{aligned}$$

就可得出结论说, 如果 m 为偶数, 则 p 除尽 $(m!)^2+1$. 费马可能偶然地, 至少是实验地, 发现了威尔逊定理的那个结论; 这也并非绝对不可能. 莱布尼茨在 1682 年左右就几乎发现了它 (参看 D. Mahnke, 引文同上, p. 42). 想象费马按照上面所描述的方式进行推理是否有点太离奇了?

我们对于莱布尼茨的了解比之于对费马的了解要多得很多, 这显然是因为莱布尼茨总是把出现在他脑海里的思想立即写下来, 并且保存了他所写下的每一片纸 (参看 D. Mahnke, 引文同上, pp.29–30). 这不是费马的习惯做法.

§2.8 两个平方数之和

在此, 如果我们让自己使用现代概念的话, 那么我们就会引进高斯环 $\mathbb{Z}[i]$; 它由 “复整数” $a+bi = a+b\sqrt{-1}$ 构成, 其中 a 和 b 是普通的整数; 像在附录 I 中将要解释的那样, 在此环内成立 “欧几里得辗转相除法”, 由此便可推出其中的每个数可以唯一地分解素因子. 那么, 已知每个普通的素数 $p=4n+1$ 除尽某个和 $a^2+b^2=(a+bi)(a-bi)$, 而却没有素数 $p=4n-1$ 除尽它, 则可以得出结论说, 后者在 $\mathbb{Z}[i]$ 中仍然是素数, 而前者不是. 于是, 如果 $r+si$ 是 $p=4n+1$ 的素因子, 则 p 必须等于 r^2+s^2.

在他 1572 年的书《代数》中, 邦贝利给予数 $a+bi$ 的理论一个说明, 即便从现代的观点看, 它也是完美的 (参看前面的第一章 §12); 但没有证据表明费马研读过邦贝利, 而且 “虚数” 似乎总处在他的视野之外. 甚至到了下一个世纪, 在欧拉多年来处理与分析相关的这些复数之后, 只是在其生命后期他才将这些数引进了数论 (参看第三章 §14). 当费马在 1640 年圣诞日写信给梅森, 告诉他说, 每个素数 $p=4n+1$ 是一个且是唯一的一个两个平方数的和时 (*Fe.*II,213; 参看 *Fe.*I,293, Obs.VII), 自然他必定已经按不同的方式在进行了. 幸运的是, 他在给惠更斯的 1659 年通信中给了他的方法的一个模糊的提示 (*Fe.*II,432; 参看下文的 §10). 在那里他说, 他用到了他的 “下降法”, 证明, 即如果对于某些素数并非如此, 则对于某些更小的素数也不如此, “ 一直下去, 直到你达到了 5 ”. 这好像

并没有使惠更斯弄明白; 我们则要好些, 因为欧拉在 1742 年到 1747 年间构造了一个完全是这种类型的一个证明 (参看第三章 §9); 这使得我们可以将这个方法从本质上说算到费马的头上, 看起来这有某种真实性. 实际上这个方法具有我们在上面所叙述使用高斯环方法的关键之处. 它或多或少像下面那样进行.

取一个素数 $p = 4n+1$; 我们已知它除尽某个和 a^2+b^2, 其中 a, b 与 p 互素. 设 r 为 a 除以 p 的余数; 如果 $r \le 2n$, 则令 $a' = r$; 否则 $0 < p-r \le 2n$, 则令 $a' = p-r$. 同样, 由 b 构造 b', 并用 a', b' 代替 a, b. 在这些完成之后, p 仍然除尽 a^2+b^2, 而 a, $b > 0$ 且 $< p/2$, 从而 $a^2+b^2 < p^2/2$ (这一步相应于对 $\mathbb{Z}[i]$ 使用欧几里得辗转相除法). 如果我们除 a, b 以它们的 g.c.d., 我们则可设它们互素. 现在记 $N = a^2+b^2$; 那么 N 除 p 以外的因子全都 $< p/2$, 于是要么是 2 要么具有形式 $4m+1$; 我们必须证明, 如果他们全都是两个平方数的和, 则 p 也是的. 到此, 欧拉发现可以有两个不同的方式做下去.

首先, 借助于基本恒等式

$$(1) \qquad (a^2+b^2)(x^2+y^2) = (ax \pm by)^2 + (ay \mp bx)^2$$

(参看第一章 §6), 我们知道, 如果 N/p 的所有素因子都是两个平方数的和, 那么 N/p 也是. 因此, 记 $N/p = x^2+y^2$, 则有

$$p = \frac{a^2+b^2}{x^2+y^2} = \left(\frac{ax \pm by}{x^2+y^2}\right)^2 + \left(\frac{ay \mp bx}{x^2+y^2}\right)^2,$$

故 p 是两个有理数的平方和. 它把我们带回到了费马在 1636 年曾提出过而显然没能解决的一个问题上 (参看前面的 §5 和第三章的附录 II).

按照欧拉的方法 (*Corr.*I,416–417,419), 我们现在以一种不同的方式来完成这个证明. 为简便计, 在这一节及下一节中, 我们称一对和为 N 的整数平方为 N 的一个 "表示". 如果两个整数 N, N' 具有表示 $N = a^2+b^2$, $N' = x^2+y^2$, 那么恒等式 (1) 的右端定义了 NN' 的两个表示, 我们这时可以说它是由 N 和 N' 的表示通过 "复合" 导出的. 欧拉的主要步骤现在可阐述于下:

引理 2. 对任意 $N = a^2+b^2$, 设 $q = x^2+y^2$ 是 N 的一个素因子. 于是 N/q 有表示 u^2+v^2 使得表示 $N = a^2+b^2$ 是一个由它和 $q = x^2+y^2$ 经复合导出的数.

将 (1) 用于 N 和 q. 我们有

$$(2) \qquad Nq = (ax \pm by)^2 + (ay \mp bx)^2.$$

但 q 除尽数

$$Ny^2 - b^2q = a^2y^2 - b^2x^2 = (ay-bx)(ay+bx),$$

从而除尽 $ay \mp bx$ 中的一个. 因此, 如果在 (2) 中选取适当的符号, 则 q 除尽左端及右端的第二项, 从而除尽第一项. 选取同一个符号, 我们则可写出

$$(3) \qquad ax \pm by = qu, \quad ay \mp bx = qv;$$

用 q^2 除 (2) 得到 $N/q = u^2 + v^2$. 由 (3) 解出 a 和 b, 给出了

$$(4) \qquad a = ux + vy, \quad b = \pm(uy - vx).$$

引理得证.

像前面那样, 如果 p 是 $N = a^2 + b^2$ 的最大素因子, 其中 a, b 互素, 并且 N 的除 p 以外的所有素因子都已知具有 $x^2 + y^2$ 的形式, 那么, 我们则可将引理 2 用到其中任何一个, 譬如 q 上, 这样对任意 N/q 的与 p 相异的素因子, 等等, 直到得到对 p 本身的一个两个平方数和的表达式为止. 这便完成了对费马陈述的证明, 它是由欧拉在一个多世纪之后得到的. 除去一些小的细节外, 费马的证明很可能就是这样的.

§2.9 由两个平方数和表示的数

我们知道, 一个数 N 是否是两个数 —— 不管是整数的还是有理数的, 平方和的问题源自丢番图 (参看第一章 §11–§12); 同样一个数 N 是否是一个 "数表示的" 直角三角形斜边 (hypotenuse)的问题也是如此, 此问题就是说是否 N^2 是两个整数平方和; 还有一个问题也来自他, 即是否一个数可以以不止一种方式表为两个平方数的和 (参看第一章 §6).

或许费马是第一个提到此问题的人, 他把它们记在《丢番图》,V .12_b 的边白上了 (*Fe*.I,313,Obs.XXV), 他仅仅从大意上说, $3n$ 不可能是两个平方数的和除非 3 除尽 n; 这恰好是说 -1 不是一个模 3 二次剩余. 可立即用对于 $N = 2m + 1$ 成为两个平方数和的 " 为真判别法 (the true criterion)" 的陈述得到 (*Fe*.I,314, Obs.XXVI): 充要条件是 m 应为偶数, 即 N 具有形式 $4n + 1$, 并且在 N 被最大的平方因子除后, 在此商中剩下的素因子它们自身也应具形式 $4n + 1$. 这包含在前面 §8 所讨论的结果之中.

但是从 1640 年当他已经开始在其通信中提到他着手该问题起(*Fe*.II,213–214; 参看 *Fe*.II,221–222, 以及 *Fe*.I,293–297,Obs.VII), 费马就没有只停留在 $N = x^2 + y^2$ 是否有解的问题上; 他寻求这些解的个数, 并找出解它们的方法. 无疑, 部分地出于习惯性的理由, 他对于 "斜边" 对应的问题给予了特殊的关注, 就是 N 是个平方数时的情形.

在计算一个整数 N 的 "表示" $N = x^2 + y^2$ 的个数时, 我们无需注意 x 和 y 的符号, 以及它们的次序; 这实质上与费马的用法一致; 当然他总是取 x, y 为

自然数. 如果 x 和 y 互素, 我们则称表示 $N=x^2+y^2$ 为 "正常" 的. 如果 x, y 有 g.c.d. $d>1$, 则可记 $x=dx'$, $y=dy'$, $N=d^2N'$, 从而 (x',y') 是 N' 的一个正常表示. 因此如果需要, 所有关于表示的问题都可以化成关于正常表示的问题. 这一点已经暗含在费马的做法里了. 特别地, 如果 N 有一个正常表示, 那么它的奇素因子必定全为 $4n+1$ 的形式; 同时, N 不能是 4 的倍数, 这是因为 x^2+y^2 除去 x, y 为偶数外不是 4 的倍数. 如果现在 $N=2N'$, 且 N' 为奇数, 那么 N' 的每个表示 $N'=x'^2+y'^2$ 给出了 N 的一个表示 $N=x^2+y^2$, 其中 $x=x'+y'$, $y=x'-y'$; 反之, 如果 $N=x^2+y^2$, x 和 y 必定全为奇数, 从而我们可以令 $x'=(x+y)/2$, $y'=(x-y)/2$, 从而 $N'=x'^2+y'^2$ (参看第一章 §6,(4)). 这些公式决定了在 N 的表示与 N' 的表示之间的 1-1 对应; 如果一方是个正常表示则另一方也是. 因此只要讨论奇整数的表示就足够了.

费马对此正确坚持的第一点是说, 每个形如 $4n+1$ 的素数具有唯一的表示. 实际上这立刻可由我们在 §8 中叙述成引理 2 的那个结果得到; 在此引理中取 $N=q$, 我们得到 $N/q=1=u^2+v^2$, 故 (u,v) 是 $(\pm1,0)$ 或者 $(0,\pm1)$; 于是 (4) 表明 (a,b) 在上面所解释的意义下定义了 q 的与 (x,y) 同一个表示; 这显然是正常的.

由此同一个引理现在可以推出: 整数 N 的任一表示可以由 N 的素因子分解的 "复合" 得到. 按照费马的叫法, 素数的两个平方数和的表示被称做 "本原" 的, 那么便可以说, 所有的表示都可以由本原表示按系统的步骤得到, 这里所说的系统的步骤是指复合. 这确实为费马在 "斜边" 情形, 即平方数的表示下详细阐述过的 (*Fe*.II,222); 无疑他也留意到了一般的情形. 由于他几乎不可能仅仅由反复试验来得出结论, 这让我们有了另外的推断, 即设想他曾拥有过一个像引理 2 那样的结果.

至于一个整数的表示个数, 费马有下面的陈述 (*Fe*.II,213–215; 参看 *Fe*.I,293–297,Obs.VII):

(I) 如果 p 为形如 $4n+1$ 的素数且 $r\geq1$, 则 $N=p^r$ 当 r 为偶数时, 正好具有 $r/2$ 个表示, 如果 r 为奇数则正好是 $(r+1)/2$ 个.

(II) 如果 m 为任意整数, 取除尽 m 的所有不同的形如 $4n+1$ 的素数; 设它们在 m 中的幂次分别为 α, $\beta,\cdots,\gamma$; 于是 m 正好是 h 次的一条斜边, 即 m^2 正好具有 h 个表示, 其中 h 为

$$2h+1=(2\alpha+1)(2\beta+1)\cdots(2\gamma+1).$$

包含 (I) 和 (II) 的给梅森的信所注日期为 1640 年 12 月 25 日. 只在几个月前 (*Fe*.II,202–204), 他还只能告诉罗伯瓦尔说, 一个素数 $p=4n-1$ 不能除尽两个互素的平方和 (即 -1 是模 $p=4n-1$ 非剩余), 还附带说, 他 "曾发现过的没

有什么能像这个结果的证明那样使他如此高兴”. 在不到半年的时间里他迈出了多大的步伐啊!

费马做出了上面所引的陈述, 但却没有详细说明对它们的证明; 但是人们不妨按他说的去重新构造出他的推理. 像上面说过的那样, 我们只要处理正常表示就足够了. 如果我们返回到引理 2 及其证明, 那么我们便由公式 (4) 知道如果 (a,b) 是 N 的一个正常表示, 那么 (u,v) 必定是 N/q 的一个正常表示. 它的逆也对, 我们也将它写为引理:

引理 3. 设 $q=x^2+y^2$ 为 N 的一个奇素因子; 假定 $N/q>2$ 且有正常表示 $N/q=u^2+v^2$. 设 (a,b) 和 (a',b') 为 N 的两个表示, 他们是由 (u,v) 和 (x,y) 经复合产生的. 于是 N 的这两个表示不相同; 如果 q 不除尽 N/q 则它们均为正常, 如果 q 除尽 N/q, 则其中一个为正常表示而另一个不是.

事实上, 我们有

$$a=ux+vy,\ b=uy-vx;\ a'=ux-vy,\ b'=uy+vx.$$

显然 $a\neq\pm a'$, 并且容易看出 $a\neq\pm b'$. 我们有

$$ax+by=uq,\ ay-bx=vq,$$

另外对 a',b' 也成立类似的公式; 由于 (u,v) 为正常, 故除了 q 外没有素数能除尽 a 和 b , 或者 a' 和 b'. 如果 q 同时除尽 a 和 a', 那么它就会除尽 $a+a'$, $a-a'$, 从而除尽 u 和 v; 因为这是不可能的, 故或者 (a,b) 或者 (a',b') 必为正常. 如果, 譬如, q 除尽 a 和 b, 那么 q^2 则除尽 $N=a^2+b^2$ 从而除尽 N/q; 因此, 如果 q 除尽 N/q, 我们就像在引理 2 的证明中那样记

$$bb'=u^2y^2-v^2x^2=\frac{N}{q}y^2-v^2q;$$

这是 q 的倍数, 故 q 除尽 b , 从而也除尽 a (如由 $N=a^2+b^2$ 所表明的那样) 或者 b', 因而也除尽 a'. 完成证明.

费马一定或多或少地按照这样一些思路在进行证明, 对此不会有太多的疑问, 虽然说他当然不会按照这种方式来表达他的想法, 而且很可能就满足于对典型数值情形的仔细分析. 相当可能的是他是从一个素数 $p=4n+1$ 的幂 $P=p^r$ 着手的; 将引理 3 或某个相似的结果应用于这样一个幂, 立刻就可以发现它有且只有一个正常表示; 它实质上等价于费马的陈述 (I). 如果现在 N 是 ρ 个不同素数的幂 $P_1,P_2,\cdots,P\rho$ 的乘积, 则此引理表明它具有 $2^{\rho-1}$ 个正常表示, 其中的这些表示都是由因子 P_i 经复合产生的, 这是因为每加一个因子就对正常表示

的个数乘上了 2; 容易由此事实推出陈述 (II). 我们也可得到对于任意整数的表示个数的公式, 不管是不是正常表示均可; 但是这就不会像 (II) 那样简单了.

我们必须在这里指出上述结果的一个推论, 因为它将在费马以后关于丢番图方程的某些工作中发挥作用 (参看下文的 §16); 我们将它叙述为一个引理.

引理 4. 设 N^3 是具有正常表示 $N^3 = a^2 + b^2$ 的一个立方数. 于是 N 具有表示 $u^2 + v^2$ 使得 $a = u^3 - 3uv^2$, $b = v^3 - 3vu^2$.

由于 N^3 有一个正常表示, N 必定为奇数也必定是 ρ 个不同形如 $4n+1$ 的素数的幂 $P_1, \cdots, P_\rho$ 的乘积; 于是 N^3 也是如此, 并且它们都具有 $2^{\rho-1}$ 个正常表示, 而这些表示均来自因子 P_i, (分别地, P_i^3) 表示的复合. 因此, N^3 的每个正常表示必定由 N 的一个且只有一个表示复合而成; 特别地, N 必定有一个表示 (u, v) 使得, 当它首先与自己复合然后与所得到的 N^2 的表示再复合, 则得到 N^3 的一个给定的 (a, b). 如果适当地选取 u, v 的符号便可得到引理中的公式. 我们也可利用高斯整数环 $\mathbb{Z}[i]$ 更加容易地得到一样的结果 (参看附录 I). 当然我们对于任意幂 N^r, $r \geq 2$ 都有类似的结果. $r = 2$ 的情形恰好是欧几里得关于毕达哥拉斯三角形的引理 (参看第一章 §5) 而不要求对于引理 4 那样精心构造的手段.

只要涉及 "复合" (即非素) 整数, 那么就可以把数的平方和的表示理论视为其全部本质所在. 所剩下的问题实际上是找出费马称作的本原表示, 即那些素数 $p = 4n + 1$ 的表示. 1654 年, 他告诉帕斯卡他已经找到对此的一个系统的解法 ("*une régle générale*": *Fe.*II,313; 参看下文的 §13). 但在 1641 年, 他还不知道有这样的方法, 那时除了反复试验 ("*tâtonner*": *Fe.*II,223) 外也没有更好的办法了.

值得注意的是, 费马 (如他所说) 在 1640 年圣诞节当天仍在 "匆匆行笔", 而他依旧有时间指出, 在形如 $X^2 + Y^2$ 的表示个数与形如 $X^2 - Y^2$ 的相似个数之间的类同, 这里所谓的相似个数更准确地说是指 N 可写为 $x - y$, 其中 xy 为平方数. 这个条件给出了 $x = du^2$, $y = dv^2$, $N = d(u^2 - v^2)$, 其中 d 是 x 和 y 的 g.c.d., 因而 u 和 v 互素. 对于 N 为奇数, 该问题解的个数除了应将 N 的所有素因子考虑在内而不仅仅是那些形如 $4n + 1$ 的以外, 的确是由 (II) 中一样的公式给出. 在其他的场合也提到过同一个问题 (*Fe.*II,256–258, 标记了两个日期), 这次是与分解大数的方法有关. 取 N 为一大的奇整数, n 为 $< \sqrt{N}$ 的最大整数. 分解 N 的传统方法是连续不断地试着将 3 到 n 的所有素数一个接一个去除它. 费马代之而起的则是力图将其写成 $N = x^2 - y^2$: 由于必定有 $x > n$, 故此可以以写出序列

$$(n+1)^2 - N,\ (n+2)^2 - N,\ (n+3)^2 - N, \cdots$$

的办法来进行, 直到出现一个平方数为止. 此序列相邻两个数的逐次差为 $2n+3, 2n+5, \cdots$, 这个计算如费马的例子所显示的那样, 容易进行下去:

$$N = 2027651281,\ n = 45029,$$

他发现

$$N = 45041^2 - 1020^2 = 46061 \times 44021.$$

如果 n 靠近 $\sqrt{N}$, 则这个方法十分奏效. 作为测试一个已知大数是否是个素数的工具, 费马在 1659 年给惠更斯的信里不得不承认它远非完美 (*Fe.*II,435), 尽管他也说他还发现了许多简便的方法. 当然在费马之后这方面取得了一些进展, 但有趣的是我们看到, 那个想象的 "坚不可摧" 的密码如今却是建立在极大数分解的假定之上的, 它超过了我们最精心设计的计算机的能力.

§2.10 无限下降法以及方程 $x^4 - y^4 = z^2$

在 1659 年通过卡尔卡维转交给惠更斯的那个简短得令人不安的关于他的数论工作的报告 (*Fe.*II,431–436= *Huy.*II, 458–462) 中, 费马对他的早期工作说了以下的话:

" 由于在书中可以找到的那些常规的方法对证明这些困难的命题已不适用, 我最终找到了一个最奇特的方法…… 我称它为无限下降法 (*infinite descent*). 最初我只用它证明否定性的结果, 诸如: '没有形如 $3n-1$ 的数可以写为 x^2+3y^2', '不存在数的直角三角形其面积是个平方数'…… 将它用在肯定性的问题上要难得多, 故而, 当我必须证明 '每个形如 $4n+1$ 的素数是两个平方数之和' 时, 我发现自己处在令人遗憾的困境之中 (*en belle peine*). 但最终这样的问题被证明是可以顺从于我的方法的……"

费马在将他的无限下降法介绍给惠更斯时所包含的第一个陈述是关于数 $3n-1$ 的, 这纯粹是个疏忽吗? 是否我们所看到的是个抄印错误? 要知道, 我们的文本根据的不是费马的手稿而是惠更斯的抄写本. 在写它的那个时候, 费马长期以来就知道 (惠更斯也的确非常清楚) 所说的这个陈述可以由模 3 的一个平凡的同余式论证得到 (参看前面的 §5); 在费马还不曾注意到此事前, 这中间还有一段时间 (参看前面的 §5); 人们难道应该想象成, 在他意识到用一个同余式的证明就足够之前, 他所做出对那个陈述 (或许还有关于两个或四个平方数和的陈述) 的第一个证明用的就是无限下降法? 然而这就有可能是, 上面这一段引述表明他对第二个陈述的证明必定在他 1640 年关于两个平方和的工作之前了 (参看前面的 §9). 而这一部分的被他给梅森的信 (*Fe.*II,65, 按推测, 标注日期

应为 1638 年; 参看前面 §2) 所证实, 在此信中他向 Sainte-Croix 提出了挑战: 要找出一个直角三角形是一个平方数、一个立方数等于两个立方数之和等等; 显然他必定已经知道, 或者至少已怀疑到这是些没有解的问题. 1640 年, 他通过梅森给了弗莱尼柯同一个 (以及另外一个不可能解的) 问题, 目的在于测试一下弗莱尼柯在这方面的理论知识: 费马告诉梅森,"如果他说在这样或那样的范围内没有解的话, 那么可以确信他在用列表的方式进行". 没有任何迹象表明弗莱尼柯给出过回答.

弗莱尼柯在他的《论数的直角三角形 (*Traité des triangles rectangles en nombres*)》(在其身后的 1676 年出版, 并于 1729 年重印, *Mém.Acad.Sc.*t.V. pp.127–206) 中, 的确放进了一个证明, 指出一个毕达哥拉斯三角形的面积既可以不是一个平方数也可以不是一个平方数的二倍. 由于费马对惠更斯所说的那个陈述 (*Fe.*II,436), 我们完全可以设定他的这个证明基于了来自费马的一封信. 因作者没能看到作品的最终出版而没有写一份鸣谢词, 这并不能表明弗莱尼柯宣称了那些证明归属于他. 在这同一本书中, 弗莱尼柯以 "归纳法", 也就是实验作为唯一的理由, 认定了每个形如 $4n+1$ 的素数是两个平方数之和 (参看下文的 §11(ii)); 我们对他所有的了解表明, 他是一个善于实验的学者, 相对照地, 费马的主要兴趣则是在理论方面的.

在写给惠更斯关于他对于毕达哥拉斯三角形面积定理的下降法证明时, 费马对该方法的叙述仅仅说道: "如果这种三角形的面积是一个平方数, 那么就会有一个更小的具有同样性质的这种三角形, 等等, 这是不可能的", 他又加了一句说 "要解释为什么他的论述过于冗长, 谜底在于其方法正完全基于此" (*Fe.*II,432). 所幸, 恰好有一次他发现在《丢番图》的最后的一个命题那里还有一块空白边可以写出这个谜底 (*Fe.*I,340–341, Obs. XLV); 它是如下进行的.

任取一个毕达哥拉斯三角形并设其边 (长) 互素; 于是可将它们写为 $(2pq, p^2-q^2, p^2+q^2)$, 这里的 p, q 互素, $p>q$, $p-q$ 为奇数 (参看第一章§5). 它的面积为 $pq(p+q)(p-q)$, 其中的每个因子均与其他的三个因子互素; 如果这是一个平方数, 则其所有的因子也必为平方数. 记 $p=x^2$, $q=y^2$, $p+q=u^2$, $p-q=v^2$, 这里的 u, v 必为奇数且互素. 于是 x, y 和 $z=uv$ 是方程 $x^4-y^4=z^2$ 的一个解; 附带地, 我们还知道了 v^2, x^2, u^2 构成了一个公差为 y^2 的算术级数中的三项 (参看第一章 §7, 以及 *Fe.*II,65, 问题 4°). 我们有 $u^2=v^2+2y^2$; 将它写成 $2y^2=(u+v)(u-v)$, 并看到 $u+v$ 和 $u-v$ 的 g.c.d.为 2, 那么我们便知它们中的一个必定具有形式 $2r^2$ 而另一个则具有形式 $4s^2$, 故而我们可将其写成 $u=r^2+2s^2$, $\pm v=r^2-2s^2$, $y=2rs$, 从而得到

$$x^2=\frac{1}{2}(u^2+v^2)=r^4+4s^4.$$

因此 r^2, $2s^2$ 以及 x 为一个毕达哥拉斯三角形的三条边, 其面积则为 $(rs)^2$ 并且它的斜边小于原来三角形的斜边 x^4+y^4. 这便完成了用 "下降法" 的证明.

除了一点字面上的更动外, 弗莱尼柯忠实地遵循了这个证明 (索引同上,pp. 173–175). 至于面积是二倍平方数的三角形, 他是如下进行的 (同上,pp.175–176). 像前面那样, 我们可记 $p+q=u^2$, $p-q=v^2$, 并且或者 $p=x^2$, $q=2y^2$, 或者 $p=2x^2$, $q=y^2$. 因为 u, v 为奇数, 而 $2p=u^2+v^2$, 故 p 必为奇数, 从而我们可记 $p=x^2$, $q=2y^2$. 于是, $4y^2=(u+v)(u-v)$; 由于 $u+v$ 与 $u-v$ 的 g.c.d.为 2, 我们则可记 $u+v=2r^2$, $u-v=2s^2$, $u=r^2+s^2$, $v=r^2-s^2$, 最终有

$$x^2=\frac{1}{2}(u^2+bv^2)=r^4+s^4.$$

于是三角形 (r^2,s^2,x) 具有面积 $2(rs/2)^2$, 从而得证.

如弗莱尼柯所看到的, 亦如费马已必定知道的那样, 由此可得到一系列的结果. 譬如, 方程 $x^4\pm y^4=z^2$ 没有平凡解的事实便包含在上述的证明之中 (参看 *Fe.*I,327,Obs.XXXIII). 还有, 在一个毕达哥拉斯三角形 (a,b,c) 中, a, b 不能同时为平方数, 这是因为这样的话, 面积 $ab/2$ 就会等于二倍的平方数; 同样, a, c 不能都是平方数, 这是因为 $a=r^2$, $c=s^2$ 的话, 就会给出 $s^4-r^4=b^2$. 由此人们可以推导出费马的陈述 (*Fe.*I,341; 参看 *Fe.*II,406), 即除 1 以外没有一个三角数是个四次幂. 三角数是指形如 $\frac{1}{2}n(n+1)$ 的数; 如果它是个四次幂, 那么整数 n, $n+1$ 中便有一个必定具形式 x^4, 而另一个则有了形式 $2y^4$, 故而我们有 $x^4-2y^4=\pm1$. 如果 $x>1$, 考虑毕达哥拉斯三角形 $a=x^2$, $b=\frac{1}{2}(x^4-1)$, $c=\frac{1}{2}(x^4+1)$; 在 $+1$ 的情形, a 和 b 为平方数, 而在 -1 的情形则 a 和 c 为平方数, 这与我们前面所证矛盾. 相似地, 考虑三角形 $a=x^2z^2$, $b=\frac{1}{2}(x^4-z^4)$, $c=\frac{1}{2}(x^4+z^4)$, 我们看出方程 $x^4\pm z^4=2t^2$ 没有非平凡解; 这或多或少是欧拉在 1738 年对此所给出的证明 (*Eu.*I–2,47–49 在 E98 中).

§2.11 费马成熟时期的问题

依然沿着费马在 1659 年给惠更斯信中所大体描述的路线走, 我们现在转回到二次剩余和二次型上; 在稍后我们会看到 (参看下文的 §16) 在研究丢番图方程中应用 "下降法" 成了费马按此方向前进的强有力的诱因.

为了马上能对当前将要讨论到的题目做一个概要的描述, 我们应注意到, 费马关于这个课题论述是在以下的标题下出现的:

(i) 关于每个整数是 "三个三角数、四个平方数、五个五角数等等之和" 的陈述; 这早在 1638 年就已断言而后则经常重复 (参看前面的 §5). 对于三角数, 它等于是说每个形如 $8n+3$ 的整数 (最多) 是三个平方数之和. 关于三个平方数

laboriosa meditatione deteximus, subiungemus; hoc nempe demonstrandi genus miros in arithmeticis suppeditabit progressus. Si area trianguli esset quadratus darentur duo quadratoquadrati quorum differentia esset quadratus: unde sequitur dari duo quadrata quorum & summa, & differentia esset quadratus. Datur itaque numerus compositus ex quadrato & duplo quadrati, aequalis quadrato, ea conditione vt quadrati eum componentes faciant quadratum. Sed si numerus quadratus componitur ex quadrato & duplo alterius quadrati eius latus similiter componitur ex quadrato & duplo quadrati vt facillime possumus demonstrare.

Vnde concludetur latus illud esse summam laterum circa rectum trianguli rectanguli & vnum ex quadratis illud componentibus efficere basem & duplum quadratum aequari perpendiculo.

Illud itaque triangulum rectangulum conficietur à duobus quadratis quorum summa & differentia erunt quadrati. At isti duo quadrati minores probabuntur primis quadratis primo suppositis quorum tam summa quam differentia faciunt quadratum. Ergo si dentur duo quadrata quorum summa & differentia faciant quadratum, dabitur in integris summa duorum quadratorum eiusdem naturae priore minor. Eodem ratiocinio dabitur & minor ista inventa per viam prioris & semper in infinitum minores invenientur numeri in integris idem praestantes: Quod impossibile est, quia dato numero quouis integro non possunt dari infiniti in integris illo minores. Demonstrationem integram & fusius explicatam inserere margini vetat ipsius exiguitas.

Hac ratione deprehendimus & demonstratione confirmavimus nullum numerum triangulum praeter vnitatem aequari quadratoquadrato.

SCHOLIVM.

Hinc patet, idem ostendi posse de quadratoquadrato ipsius 12. quod ostensum est de quadratoquadrato ipsius [illegible]. Quare verum est in quolibet triangulo rectangulo quadratum areae duplicatae additum quadratoquadrato cuiuslibet lateris circa rectum efficere quadratum. Vt in data hypothesi 24. [illegible] quadratoquadratis ipsorum 3. & 4. putà cum 81. & 256. fiunt quadrati 225. & 400. sed & conditionis adiectae necessitas per algebram sic demonstrabitur. Data area cuiuslibet trianguli rectanguli puta 6. ponatur vnum laterum circa rectum 1 N. erit alterum $\frac{12}{1N}$. Vt autem sit triangulum rationale oportet, vt summa quadratorum, putà 1 Q. + $\frac{144}{1Q}$ aequetur quadrato, & omnia ducendo in 1 Q. fit 1 QQ. + 144. aequalis quadrato. Vnde patet quadratoquadratum cuiuslibet lateris circa rectum adiecto quadrato areae duplicatae, debere conficere quadratum.

Porro hanc ipsam quaestionem tractans Franciscus Vieta Zeteticorum libri quarti, duas alias ei praefigit conditiones. Prima est. Oportet vt area addendo aliquem quadratoquadratum, fiat quadratoquadratus, vel vt ducendo aream in aliquem quadratum, & productum addendo alicui quadratoquadrato, fiat quadratoquadratus. Et haec conditio, sufficiens quidem est, vt demonstrat Vieta, sed an sit necessaria merito quis ambigat. Sanè arbitror eum eius necessitatem demonstrare non posse [illegible] secundam excogitasse. Secunda conditio est. Oportet vt datus areae numerus, sit cubus suo multatus latere, vel vt idem per quadratum aliquem multiplicatus, sit cubus suo multatus latere. Et haec conditio non solum sufficiens est, vt ostendit Vieta, sed etiam necessaria vt demonstrabimus, [illegible] laborare videatur. Quamuis satius sit hanc conditionem ita proponere. Oportet vt areae numerus sit cubus suo multatus latere, latusve suo multatum cubo. Vel vt eo per aliquem quadratum multiplicato [illegible], sit cubus suo multatus latere, latusve suo multatum cubo. Huius autem ratio est, quia quodlibet triangulum rectangulum, potest concipi simile alteri triangulo, quod formatum sit ab vnitate, & ab alio quouis quadrato, cuius quadrati si ponas latus 1 N. fiet trianguli hypotenusa 1 Q. + 1. alterum laterum circa rectum 2 N. alterum 1 Q. − 1 vel 1 − Q. prout 1 N. supponitur maior vel minor vnitate. Quare fit area 1 C. − 1 N. vel 1 N. − 1 C. ita si fingas triangulum ab 1. & 4. modo tradito [illegible] porismatum. Fient latera 3. 4. 5. Area vero 6. cubus scilicet 8. suo multatus latere. At si formes triangulum ab 1. & $\frac{1}{4}$. fiet triangulum [illegible], cuius area [illegible] est latus $\frac{1}{2}$ multatum suo cubo.

Proposito vero quolibet alio triangulo, cum per quartam tertij porismatum, necesse sit illud formari à duobus planis similibus, hos planos [illegible], & vtrumque per numerum ipsorum [illegible] diuidens, fient duo quadrati in eadem ratione, quorum minor erit vnitas, à quibus si formes triangulum, erit

费马的下降法

之和的其他陈述出现在 1658 年给迪格比 (*Fe*.II,405) 以及在《丢番图》的一个边白注记上 (*Fe*.I,314–315,Obs.XXVII), 它具有属于费马事业初期时的全部形态. 参看下文的 §14.

(ii) 早在 1641 年, 费马似乎就已注意到二次型 X^2-2Y^2 的某些主要性质了 (参看 *Fe*.II,221,224–226); 弗莱尼柯也显然留意到了 (参看 *Fe*.II,231–241), 但他在他的《论数的直角三角形》(索引同上) 中所详细论述的结果却是通过 "归纳" 即实验得到的. 弗莱尼柯在这方面的启迪主要来自对毕达哥拉斯三角形的研究; 他在形式 X^2-2Y^2 方面的兴趣是由如下的事实产生的, 即一个所谓的 "本原" 三角形

$$(a,b,c)=(2pq,p^2-q^2,p^2+q^2)$$

(也就是说一个 a,b,c 互素的直角三角形; 参看第一章 §5) 的两条直角边的和与差由以下形式给出:

$$|b\pm a|=|p^2-q^2\pm 2pq|=|(p\pm q)^2-2q^2|.$$

至于对费马, 人们得到的印象是, 他立即就被二次型吸引过去了.

(iii) 现存的费马与弗莱尼柯的通信, 包括经由梅森转交的, 全部集中于 1640 年到 1641 年间. 自此以后直到 1657 年弗莱尼柯的名字尽管也出现但在费马的信中却极为罕见. 的确, 只要瞄一眼他的《全集》的第二卷就会明白, 他在 1642 年到 1654 年间的通信中几乎没有提出关于数学方面的内容. 只有到了 1654 年我们才第一次了解到, 在这些年里费马在数论方面所取得的进展; 在与帕斯卡交换关于概率论方面的一些信 (它们是极为重要的, 但与我们这里要说的无关) 后, 费马鼓起足够的自信寄给了帕斯卡他在 "数" 方面的发现 (*Fe*.II,312–313). 这里新的、第一次出现的是二次型 X^2+3Y^2, X^2+2Y^2, 同时提到的还有求形如 $4n+1$ 的素数表示 $p=a^2+b^2$ 的两个平方数的 "普遍法则". 我们在前面所提到的《丢番图》的边注中发现了二次型 $X^2\pm XY+Y^2$ (*Fe*.I,300–301,Obs.X–XII), 但是正如下面所表示的, 自然不能把它与 X^2+3Y^2 孤立开来看:

$$4(x^2\pm xy+y^2)=(2x\pm y)^2+3y^2,$$

$$x^2+3y^2=(x\mp y)^2\pm 2y(x\mp y)+(2y)^2.$$

对于费马所说的这些二次型, 他已经证明了如下一些事实: 每个形如 $3n+1$ 的素数可以写成 x^2+3y^2 的形式 (*Fe*.II,313,403; 参看 *Fe*.I,301,Obs.XII); 每个形如 $8n+1$ 或 $8n+3$ 的素数均可写为 x^2+2y^2 的形式 (*Fe*.II,313,403); 每个形如 $8n\pm 1$ 的素数均可以无限多种方式写成 $|x^2-2y^2|$ (*JEH*. 41). 后面的这个结果已为弗莱尼柯所知 (实验型的, 参看前面的 (ii)) ; 在他给费马的 1641 年的信中有所叙述 (*Fe*.II,235).

(iv) 1654 年, 费马想要唤起帕斯卡对于数论的兴趣的企图显然失败了. 1656 年, 英国冒险家, 双重身份代理商 K. 迪格比 (伊夫林*19 给他的称号是 "臭名昭彰的江湖骗子", 而同时代的另一个人则称其为 "我们时代谎言方面的绝对普林尼"*20) 造访了图卢兹; 显然他必定在这样或那样的场合会见过费马, 费马从他那里收到了沃利斯的《无穷的算术 (*Arithmetica Infinitorum*)》, 这是在 1656 年出版的 (参看 *Fe.*II,337, 以及前面的 §3). 这件事重新复活了费马要找到一个值得与其争辩切磋的友好对手的希望; 他与迪格比的通信以及他通过迪格比与英国数学家沃利斯和布龙克尔*21 (Brouncker) 的通信覆盖了从 1657 年 1 月到 1658 年 6 月的一年半的时间. 起初是以一些问题向沃利斯和布龙克尔提出挑战, 但也同时针对了弗莱尼柯和舒腾*22 (Frans Van Schooten), "以及欧洲其他所有的人", 这些问题特别着重于 (因欧拉的一个错误) 后来被称作的 "佩尔方程". 如果某个刚从印度回来的传教士告诉了费马说, 他的问题已经在几乎六个世纪前被当地的数学家成功解决, 他会怎样的吃惊啊! (参看第一章 §9.)

那些通信中包括了各式各样的丢番图方程, 有整系数的也有有理系数的; 其中一些我们在前面已经考虑过了, 譬如不存在具平方数面积的毕达哥拉斯三角形; 至于其他的容后面再谈. 在涉及二次型的这里, 我们只需注意到一个关于形式 X^2+5Y^2 的猜想; 费马通过实验观察到, 当形如 $20n+3$, $20n+7$ 的素数不能写成 x^2+5y^2 时, 任意两个这样的素数的乘积则可写成这种形式; 他提及此事时说 (*Fe.*II,405), 他相信这个事实但不能证明它. 由自拉格朗日以来所知的结果看 (参看 *Lag.*III,775–776), 这正是该由类数登场的情形了. 怪不得这使费马感到了困惑!

(v) 最后, 在 1659 年与惠更斯的通信中, 当费马重复着上述的一些陈述时, 他还指出了他关于丢番图的 "单个和二重方程" 方面的工作. 它们中的大多数都引向了亏格为 1 的曲线 (参看下文的 §15); 但是费马给出了两个属于二次型的例子. 他说, 譬如举方程 $2x^2+7967=y^2$ 为例; "我有一个一般的法则, 当它可解时便能解出它, 否则则可发现它不可解, 而且不管其系数如何我都可以做到"; 对此他还进一步添加了另一个例子[7], "二重方程" $2x+3=y^2$, $3x+5=z^2$, 它

[7] 在 *Fe.*II,435, 第 2 行的 $2N+5$ 是 $3N+5$ 的一个排版错误 (参看 *Fe.*IV,140, 第 2 行, 以及 *Huy.*II,461, 第 10 行). 至于第一个方程 (*Fe.*IV,139, 倒数第 2 行), 应以 1967 替代 7967; 这对于正确阅读的影响极小; 我们应注意到有 $7967=31\times257$ 而 $1967=7\times281$.

*19 J. Evelyn,1620—1706, 英国乡绅、著作家、皇家学会创始人之一, 有关于美术、林学、宗教方面大量著作.

*20 Pliny, 古罗马时的博物学家.

*21 1620—1684, 爱尔兰数学家, 但为伦敦皇家数学会第一任会长; 主要工作是关于连分数以及用无穷级数计算对数方面.

*22 1615—1660, 荷兰数学家, 以推广笛卡儿的解析几何而知名.

相当于 $2z^2-3y^2=1$. 提及丢番图表明费马在此所要求的是 "分式解", 即有理解. 换句话说, 他所指的一般性问题是拉格朗日在 1768 年成功处理了的那个求任意方程 $x^2=Ay^2\pm Bz^2$ 整数解的问题.

§2.12 "初等" 二次型

现在我们便着手讨论前面 §11 所列出的话题; 先从 (iii) 和 (ii) 开始.

在第一章 §8 中, 我们曾叙述过作为古代来源的两个公式 (5) 和 (6); 这里只要将它们写成如下的形式就够了:

$$(5)\qquad (x^2+Ay^2)(z^2+At^2)=(xz\pm Ayt)^2+A(xt\mp yz)^2,$$

其中 A 为可正可负的整数; 从一种情形转移到另一种情形会造成困难的时代早已不复存在了. 费马洞悉这个观点, 但对于其同时代的人却没有几人能如此; 他们更愿意将 (5) 看作是特殊情形 $A=1$ 的显然推广.

在 §7,§8,§9 中, 我们曾借助于欧拉的工作力图重新构造出费马的有关两个平方数和的过程, 在那里他运用了引理 2 (§8) 和引理 3 (§9). 现在仍然按照欧拉的办法, 我们注意到, 如果除了以形式 X^2+AY^2 替代 X^2+Y^2 外, 无需改动证明而引理 2 依旧有效. 当然, 此时的复合应理解为是基于恒等式 (5) 的. 对于 (3) 和 (4), 我们必须作变换

$$ax\pm Aby=qu,\qquad ay\mp bx=qv,$$
$$a=ux+Avy,\qquad b=\pm(uy-vx).$$

由此推广了引理 2, 我们如同在 §9 中所做的那样得到: 如果 $A>1$, 一个素数 q 不能以一种以上的方式写成 x^2+Ay^2 的形式; 因为如果可以的话, 将我们的结果用到 q 以及用到 $N=q$ 就会给出 $1=u^2+Av^2$. 另一方面, 如果 A 为负数, 则同一论述则马上引向了佩尔方程; 这将在 §13 中更详细讨论.

如在 §8 中那样, 我们再一次由此引理得到: 如果一个素数 p 除尽数 $N=a^2+Ab^2$, 并且如果 N 的每个其他的素因子可以写成 x^2+Ay^2, 则 p 也具有此形式. 借助于此, 我们重新考虑在 §8 中对于形式 X^2+Y^2 的那个证明. 我们暂时采用一下欧拉的术语: 称一个奇素数 p 为一个 "公式" (或者 "形式") X^2+AY^2 的素因子是说它除尽某个整数 $N=a^2+Ab^2$, 其中 a, b 均与 p 互素; 这样的 p 的充要条件是 $-A$ 为模 p 的二次剩余 (参看 §7). 设 p 为这样的一个素数; 取 a, b 为与 p 互素的整数使得 p 除尽 a^2+Ab^2. 设 r 为 a 除以 p 的余数, 并令 $a'=r$ 或 $p-r$, 按其中最小者决定; b' 按相似地定义由 b 得到, 那么, 我们可将 a, b 以 a', b' 替换, 而后再将 a', b' 除以它们的 g.c.d.; 换句话说, 我们可以假定 a, b 互

素且 $< p/2$. 令 $N = a^2 + Ab^2$. 如果 $A = 2$, 我们有 $N < 3p^2/4$, 故而 N 除 p 以外的所有素因子均 $< 3p/4$; 于是, 完全同于 §8, 我们运用 "完全归纳法" 可假定它们全都可以写成 $x^2 + 2y^2$ 的形式 (注意, 如果 N 为偶数则这也包含了素数 2), 应用引理 2, 我们便知道 p 也可写成这种形式. 取 $A = 3$, 于是有 $N < p^2$, 因此当 N 为奇数时成立同样的推理. 如果 N 为偶数, 则 a, b 必为奇数, 并且如果适当地选取符号我们便有 $a \equiv \pm b \pmod 4$. 于是 $a' = \frac{1}{4}(a \pm 3b)$ 以及 $b' = \frac{1}{4}(a \mp b)$ 均为整数, 从而 $N/4 = a'^2 + 3b'^2$ 也是整数; 因而如有必要, 我们可用 $N/4$ 代替 N 等诸如此类的, 直到我们将 N 换成了一个具有同样性质的奇素数为止. 因此, $X^2 + 3Y^2$ 的所有素因子全都可以写成 $x^2 + 3y^2$ 的形式. 对于 $A = -2$ 我们也可同样进行, 这是因为在此情形下, $0 < a$, $b < p/2$ 表明 $|N| < p^2/2$. 如上所注意到的, 表示 $p = x^2 + Ay^2$ 当 $A = 2$ 或 3 必定唯一, 但当 $A = -2$ 是则自然不是的, 这由恒等式 (5) 并结合 $1 = 3^2 - 2 \times 2^2$ 便清楚了. 附带地, 如欧拉所看出的那样, 恒等式 (5) 表明对于 $A = 1$, ± 2, 3, $N = a^2 + Ab^2$ 的所有奇因子 (不仅是所有奇素因子) 均可写为 $x^2 + Ay^2$ 的形式, 但这里的 a, b 互素.

显然, 每个整数 $x^2 + 3y^2$ 如果不是 3 的倍数则必定具有形式 $3n + 1$; 因此前面的结果表明 $X^2 + 3Y^2$ 的每个素因子即每个使 -3 为二次剩余的素数, 必定具有此形式; 要完成费马在 1654 年关于这些素数陈述的证明, 我们还必须证明它们的逆. 这是一个与在 §7 中对形式 $X^2 + Y^2$ 所指出的同一类型的难点; 再次按欧拉所做的那样, 我们记 $p = 3n + 1$ 并使用恒等式

$$x^{3n} - 1 = (x^n - 1)(x^{2n} + x^n + 1).$$

对于所有互素于 p 的 x, p 除尽它的左端; 由 §7 的引理 1 我们知道, 对于互素于 p 的一个 x, p 必除尽右端的第二个因子, 而又因

$$4(x^{2n} + x^n + 1) = (2x^n + 1)^2 + 3,$$

这表明 p 确实是 $X^2 + 3Y^2$ 的一个因子.

至于形式 $X^2 \pm 2Y^2$, 先取 $p = 8n + 1$ 并且写出

$$x^{8n} - 1 = (x^{4n} - 1)\left((x^{2n} \mp 1)^2 \pm 2(x^n)^2\right).$$

如上所做, 使用引理 1 我们得到 p 是 $X^2 + 2Y^2$ 和 $X^2 - 2Y^2$ 的一个因子. 现在设 p 具有形式 $8n - 1$ 或者 $8n + 3$. 如果 $p = 8n - 1$, 那么它不可能是 $X^2 + 2Y^2$ 的一个因子, 这是因为我们已经看到过这样一个因子, 它本身就具有形式 $x^2 + 2y^2$, 从而为 $8n + 1$ 或者 $8n + 3$ 的形式. 同样的理由, 如果 $p = 8n + 3$, 则它不可能是 $X^2 - 2Y^2$ 的因子. 现在根据 §7, 在这两种情形下, p 都不是 $X^2 + Y^2$ 的因子; 因

此, 如果令 $p=2m+1$, 以下 $2m$ 个整数

$$1^2,2^2,\cdots,m^2,-1^2,-2^2,\cdots,-m^2$$

中任意两个都不可能是模 p 同余的, 故而它们穷竭了这 $2m$ 个互素于 p 的模 p 同余类. 这表明, 对于互素于 p 的每个数 a, 整数 a 与 $-a$ 中的一个是二次剩余, 而另一个则不是. 取 $p=8n+3$; 由于 p 不是 X^2-2Y^2 的一个因子, 故 2 不是模 p 的二次剩余; 因此 -2 便是这样的剩余, 这等于是说 p 是 X^2+2Y^2 的一个因子; 于是它自己便可写成 x^2+2y^2. 类似地, 如果 $p=8n-1$, 它便是 X^2-2Y^2 的一个因子, 从而可写为 x^2-2y^2 的形式. 这样, 所讨论的费马关于二次型的陈述已证明完毕.

关于将整数用形式 X^2+2Y^2, X^2+3Y^2 表示的个数问题, 费马必定已经知道, 凡是他所依循的对于两个平方数和的方法都可以几乎无更改地应用到这里; §9 的引理 3 及其证明对于这些形式依然有效, 但需要加上当形式为 X^2+3Y^2 时有 $q>3$, $N/q>3$ 的假定. 恰如在 §9 中那样, 我们由此知道: 整数 N 的所有表示均可通过对除尽 N 的那些素数的表示的复合 (在恒等式 (5) 的意义下) 得到. 特别地, 每个整数 N^r 的正常表示均可由 N 的一个表示的复合推导出. 对于 $r=2$, 就像在两个平方数和的情形那样, 可以以初等方法予以验证 (参看前面的 §9); 事实上, 对于形式 X^2+2Y^2, 情形 $r=2$ 在我们曾于 §10 叙述过的费马的证明中起过作用. 费马至少还一定知道 $r=3$ 的情形, 这是因为它是在我们后面 §14 中将讨论的一个证明中所需要的; 我们将其在此叙述为一个引理:

引理 5. 假设 $N^3=a^2+Ab^2$, 其中 a, b 互素, 并且 $A=2$ 或 3. 于是我们有 $N=u^2+Av^2$, 其中的 u, v 使得 $a=u^3-3Auv^2$, $b=3u^2v-Av^3$.

其证明类似于 §9 中引理 4 的证明; 当然现在是基于 (5) 的. 这里, 我们还可以利用环 $\mathbb{Z}[\sqrt{-2}]$ 以及 $\mathbb{Z}[j]$ 得到一个更容易的证明 (参看附录 I).

形式 X^2-2Y^2 的情形更加复杂, 这是因为这里不得不考虑 $x^2-2y^2=\pm1$ 的解 (参看第一章 §8,§9). 在 1641 年, 费马已经对这里的一些重要事实有所了解 (参看同上的 §9(ii)), 而他的主要陈述包含在了他与弗莱尼柯的通信中了, 弗莱尼柯将它们做成几个复印本并且加到他自己 1657 年的小册子里了 (*JEH*.41–44). 那时, 他的动机是要研究方程

$$(6)\qquad (2X^2-1)^2=2Y^2-1.$$

费马在 1659 年告诉惠更斯说, 除了 $(1,1)$ 和 $(2,5)$, 它没有其他的整数解, 他还将对此的一个证明寄给了弗莱尼柯 (*Fe*.II,434=*Huy*.II,461, 以及 *Fe*.II,441=

*Huy.*II,538). 1883 年杰诺基[*23]用 (欧拉证明的, 费马也可能知道的 (参看前面的 §10)) 事实, 即方程 $X^4 \pm Y^4 = 2Z^2$ 无解, 给出了对它更加简单的证明 (*Nouv.Ann. Math.*(III)2, 306–310). 对于费马来说, 方程 (6) 是与他在 1657 年向 "英国数学家和其他所有人" 挑战的有关问题之一中出现的, 这个问题就是, 求一个立方数, 它加上它的因子和构成一个平方数. 作为例子, 他举出 7^3, 他给出 $1+7+7^2+7^3 = 20^2$ (*Fe.*II,342), 但很快他又加了一句说, 他还知道其他的解 (*Fe.* II,342).

弗莱尼柯也注意到, 如果立方数是 p^3, 其中 p 为素数, 费马的条件可写成

$$1 + p + p^2 + p^3 = (p+1)(p^2+1) = \text{一个平方数}.$$

由于 2 不是一个解, 故 $p+1$ 和 p^2+1 有 g.c.d. 2 且必为 $2x^2$, $2y^2$ 的形式, 其中 (x, y) 是方程 (6) 的一个解. 弗莱尼柯不能证明没有这样的素数, 但是不知以何种方式发现在 7 与 10^{75} 之间没有这样的素数 (参看 *Huy.*II,25 以及 *JEH.* 23–24). 因此, 在处理 (6) 时, 费马特别更多地关注 $p = 2x^2 - 1$ 为素数的情形. 他是如下这样进行的.

由每个正或负的整数 n 的以形式 $X^2 - 2Y^2$ 的表示 $n = x^2 - 2y^2$, 我们用 "复合" 推导出 $-n$ 的表示

$$-n = (x \pm 2y)^2 - 2(x \pm y)^2;$$

这只不过是 (5) 的 $A = -2$, $z = t = 1$ 的情形 (参看第一章§8). 因此, 在处理那个形式时, 只要考虑或者是正的或者是负的整数就够了. 部分地是因为应用了 (6), 费马将自己只局限于后者, 即对正整数 n 的表示 $n = 2y^2 - x^2$, 其中他自然取 x, y 为正整数, 我们也将这样做; 于是 $0 \leq x < y\sqrt{2}$. 还是用复合, 即将 (5) 应用于 $A = -2$, $z = 3$, $t = 2$ 的情形, 我们便看出下面两个变换

$$(7) \qquad (x, y) \mapsto (|3x - 4y|, 3y - 2x),$$

$$(8) \qquad (x, y) \mapsto (3x + 4y, 3y + 2x),$$

其中的任一个都将 $n = 2y^2 - x^2$ 的一个表示变换成另一个. 费马由此观察到, 总存在一个使得 $0 \leq x \leq y$; 事实上, 如果 $x > y$, (7) 将 (x, y) 变换成 (x', y'), 使得 $x' < x$, $y' < y$, 故而按需要迭代 (7) 我们便到达某个表示 (x_0, y_0) 使得 $x_0 \leq y_0$; 费马称此表示为 "*le plus petit couple*(最小偶对)"; 我们则称其为极小 (*minimal*). 将 (7) 再次用于它, 便得到一个表示 (x_0', y_0') 使得 $x_0' \geq y_0'$, $x_0' \geq x_0$, $y_0' \geq y_0$; 将 (8) 反复地应用于 (x_0, y_0) 和 (x_0', y_0'), 我们得到同一个整数 n 的两个表示的序

[*23] Anglo Genocchi, 1817—1889, 律师、政治活动家、数学家, 主要兴趣为数论, 以 Genocchi 数而知名.

intervallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis unitatibus 10. aequatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quaestioni.

[illegible]

IN QVAESTIONEM VII.

CONDITIONIS appositae eadem ratio est quae & appositae praecedenti quaestioni, nil enim aliud requirit quam ut quadratum intervalli numerorum sit minus intervallo quadratorum, & Canones iidem hic etiam locum habebunt, ut manifestum est.

QVAESTIO VIII.

PROPOSITVM quadratum dividere in duos quadratos. Imperatum sit ut 16. dividatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. aequales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot unitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. haec aequabuntur unitatibus 16 − 1 Q. Communis adiiciatur utrimque defectus, & a similibus auferantur similia, fient 5 Q. aequales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$. & utriusque summa est $\frac{400}{25}$. seu 16. & uterque quadratus est.

[illegible]

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVAESTIO IX.

RVRSVS oporteat quadratum 16 dividere in duos quadratos. Ponatur rursus primi latus 1 N. alterius vero quotcunque numerorum cum defectu tot unitatum, quot constat latus dividendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille vero 4 Q. + 16. − 16 N. Caeterum volo utrumque simul aequari unitatibus 16. Igitur 5 Q. + 16. − 16 N. aequatur unitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

[illegible]

Hiij

费马的“大定理”

列 (x_i, y_i) 和 (x'_i, y'_i), 它们之间互不相同除非 $x_0 = 0$ 或者 $x_0 = y_0$. 费马由此正确地得出结论说, $n = 2y^2 - x^2$ 的每个解可以从极小解通过这个过程推导出来; 他写道, "所有这一切的证明都很容易", 虽说挑剔的读者觉得有个详细阐述会更好些. 对于现代的读者而言, 最好的方法是放在环 $\mathbb{Z}[\sqrt{2}]$ 中考虑, 这样便能将问题弄清 (参看附录 I); 记 $n = 2y^2 - x^2$ 等同于记 $-n = N(\xi) = \xi\xi'$, 其中 $\xi = x + y\sqrt{2}$, $\xi' = x - y\sqrt{2}$; 变换 (8) 等于是 $\xi \mapsto \varepsilon^2\xi$, $\varepsilon = 1 + \sqrt{2}$, 而 (7) 等于是 $\xi \mapsto \varepsilon^{-2}\xi$ 或者 $\xi \mapsto -\varepsilon^2\xi'$, 按情况而定; 但是几乎不能想象费马, 哪怕是试探性地, 会按这种方式来进行, 尽管欧几里得在他的 "书" X 提供了先例 (参看第一章 §8). 不管怎样, 将上面的处理应用到 $n = 1$ 以及 "极小表示" $1 = 2 \times 1^2 - 1^2$ 提供的事实是, $1 = 2y^2 - x^2$ 的所有解均可通过对一个解反复使用 (8), 即通过反复与表示 $1 = 3^2 - 2 \times 2^2$ 复合得到. 又, 通过与极小表示的复合, 它便产生了 $x^2 - 2y^2 = 1$ 的所有解, 因此证明了塞翁的 "边和对角线数 (side and diagonal numbers)" (参看第一章§8) 给出了 $x^2 - 2y^2 = \pm 1$ 的所有解.

费马进一步的推导必定是按照了他的关于形式 $X^2 + Y^2$ 的理论所建立的模式进行的, 即便如此, 也还不能说这个模式已清晰地呈现在他与弗莱尼柯的通信中了. 正如同他在证明素数 $p = 4n+1$ 可表示且唯一表示为两个平方数和 (参看前面的 §8 与 §9) 时那样, 他必定用相似的论证发现了, 任意素数以 $X^2 - 2Y^2$ 形式的两个表示必定是那些可通过与 ± 1 的一个表示复合相互推导而来的形式 (参看 §8 中引理 2 的证明, 以及前面关于把它推广到形式 $X^2 + AY^2$ 时的注释); 由上面所示, 它等于是说一个素数 p 只能具有一个极小表示 $p = 2b^2 - a^2$, $0 < a < b$. 于是, 应用复合我们由此推导出一个表示 $p^2 = 2B^2 - A^2$, 其中

$$(9) \qquad A = |a^2 + 2b^2 - 4ab|, \qquad B = a^2 + 2b^2 - 2ab,$$

容易验证它为极小. 反之, 如果 p 是个任意的奇素数, 并假定 p^2 具有表示 $p^2 = 2B^2 - A^2$; 也可假定它是极小的, 从而 $0 < A < B$; 我们于是有 $p^2 = A'^2 - 2B'^2$, 其中 $A' = 2B + \delta A$, $B' = B + \delta A$, $\delta = \pm 1$; 由于 A 必为奇数, 故可选取 δ 使得 $A' \equiv p + 2 \pmod 4$. 这给出了

$$2B'^2 = (A' - p)(A' + p),$$

由此 (就像 §10 中费马的证明那样) 我们得到的结论是, A', B', p 可以写为

$$A' = a^2 + 2b^2, \quad B' = 2ab, \quad p = 2b^2 - a^2,$$

其中 a, b 为正整数; 于是 A, B 由 (9) 给出. 另外, 如果 $\delta = +1$, 则不等式 $p > 0$, $A < B$, 而如果 $\delta = -1$ 则 $p > 0$, $A > 0$ 表明有 (当 p, A, B 均用 a, b 表示时) $a < b$, 故 $p = 2b^2 - a^2$ 是 p 的极小表示.

像在费马的问题中那样, 我们现在假设 $p = 2x^2 - 1$ 以及 $p^2 = 2y^2 - 1$; 它们分别是 p 和 p^2 的极小表示. 应用上面已经证明的事实, 即在其中取 $A = 1$ 及 $B = y$, 我们发现 A 和 B 由 (9) 给出, 其中的 $p = 2b^2 - a^2$ 是 p 的一个极小表示. 然而就像刚才所见, 一个素数 p 只能有一个这样的表示; 因此, 我们有 $a = 1$, $b = x$, 而 (9) 现在给出的是

$$1 = |1 + 2x^2 - 4x|,$$

可以清楚地看出它除了 $x = 1$ 或 2 外没有其他的解, 这给出了 $p = 1$ (这不是素数) 和 $p = 7$. 就涉及素数而言, 这已完成了证明.

尽管在我们上面所讨论的问题上费马的认识远不是那么清晰的, 人们很想辩白说, 如果他愿意的话, 他是能够补上这些缺口的. 可惜, 他与弗莱尼柯的通信的内容, 十分清晰地表明并没到此为止. 他写道: “那些对素数所证明的断言, 正如你所知, 可以被推广到复合数上…… 我不想详细阐述如此简单的东西了”. 因此他说, 方程 (6) 除了 (1,1) 和 (2,5) 外确实再没有其他解了.

但是他的论证对于 “复合” (即非素) 数不再成立, 这是因为这样的整数一般来说具有多于一个的 “极小” 表示, 这其实必定已多年来为他和弗莱尼柯所知 (参看以上所引的 §11 (ii)). 明显地, 他被自己轻率使用的 “*le plus petit couple*”, 即我们翻作 “极小” 的词给套进去了. 当然, 对于给定的 n, $n = 2y^2 - x^2$ 的最小解是 “极小” 的, 但反过来则是不对的.

没有迹象表明弗莱尼柯察觉出费马的最后那个推断的谬误之处; 1944 年当霍夫曼发表费马的文章时也没有发现它. 的确, 公正地说, 人们可以推测该证明以某种方式曾出现在他的脑海中. 但是, 至少在这种场合下, 费马的那种思维的高速度使他犯下了这个错误. 他的一些崇拜者试图为他建立的永远正确的声誉只不过是一个神话罢了.

§2.13 佩尔方程

对于形式 $X^2 - 2Y^2$ 的研究一定使得费马相信求方程 $x^2 - Ny^2 = \pm 1$ 的整数解的极端重要性, 或者用现代的说法, 即求实二次域单位元的极端重要性. 像我们已在第一章 §8–§9 看到的那样, 阿基米德和印度人早在他很久以前就走上了这条路; 当然, 他既不了解印度人的东西, 也不知道阿基米德的 “*problema bovinum*” (见第一章 §9 所讨论的警句). 他读过塞翁的东西 (*Fe.*II,266), 从而知道 “边和对角线数” (参看第一章 §8), 但这不曾超过 $x^2 - 2y^2 = \pm 1$ 的情形.

1657 年, 当费马将方程 $x^2 - 2y^2 = \pm 1$ 作为向英国和其他地区的数学家的一个挑战问题时, 他要求得到的是整数解; 而在英国进行的这场挑战中并未明确阐

明此点, 但正如在给弗莱尼柯的信中他写道, “不用说” (*Fe.*II,334), 因为只有一个新手 (“*le moindre arithméticien*”) 才会得出一个有理数解. 然而, 首先由沃利斯和布龙克尔交给他的恰是这样一个有理数的解 (*Fe.*III,418). 当费马向他们指出这并不是他原来的意思时, 他是想要叫他们承认这是他们的疏忽吗? 当在延后几个月他收到了他们的完整解答后, 是否他感到了几分烦恼? 在像通常那样通过迪格比转交的信中, 他的回答是说, 他 “欣然且愉悦地承认” 他们解答的有效性 (“*libens agnosco, imo et gaudeo...*” *Fe.*II,402). 但是, 次年在写给惠更斯的私人信件 (*Fe.*II,433) 中, 他指出这些英国人没能给出一个 “一般性的证明”. 惠更斯也对沃利斯说了同样的话 (*Huy.*II,211). 按费马的意思, 一般性的证明只能通过下降法得到.

因此可以猜测费马的求解法与他从沃利斯和布龙克尔那里得到的方法没有太大的差别[8], 但他却能够从其提取出的一个总能导出一个解的形式证明. 我们现在要概述的是沃利斯归功于布龙克尔的一个证明 (*Wal.*II,797; 更详细的内容可参看 A.Weil,*Coll.Papers.*III,413–420); 在那些通信中所叙述的证明中, 这是最令人满意的一个, 它等价于印度人的*cakravāla*(轮转法, 见第一章 §9) , 也同样等价于现代基于连分式的处理方法.

在这里我们的出发点是假定存在 $x^2 - Ny^2 = 1$ 的一个解 (x, y) , 从而逐次地将该问题化成另一个问题, 使得这些问题的每一个都有比前一个有更小的一个解; 像在费马处理具平方面积的毕达哥拉斯三角形可以看出的那样 (见前面的 §10), 这是费马的典型下降法; 事实上差别在于在后面的情形中要求的是证明无解, 而前者的目的是要找到一个解. 与此同时, 巴歇对于方程 $ac - by = \pm 1$ 的求解方法 (参看第一章§4) 无疑给沃利斯和布龙克尔提供了一个后来费马也跟进的模式, 它实际上有赖于如下的观察. 对于 $a > b > 0$, 假定方程 $aY - bX = \pm 1$ 有一个正整数解 (x, y) (全不为 0, 因为对于巴歇和他同时代的人来说, 0 不再像是 1 那样的 “数” , 这已不同于欧几里得的那个时候了); 当然 a, b 必须是互素的. 记 $a = bm + c$, 其中 $0 < c < b$, 并令 $x = my + z$. 于是我们有 $bz - cy = \mp 1$, 且 (y, z) 是方程 $bZ - cY = \mp 1$ 的一个正整数解, 它们分别小于 x 和 y; 这个方程类似于原来的方程, 顺带地具有了更小的系数. 重复这个过程, 必定最终到达了一个方程 $rV - sU = \pm 1$, 其中 $r > s > 0$, 它具有解 (u, v) 满足 $u > v = 1$; 这意味着 $r = su \pm 1$; 将此过程再向前推进一或两步, 就像一个现代数学家会做的那样, 我们便到达了解为 $(1, 0)$ 的那一步. 不管怎样, 对于最后的那个方程其解是显然

---

[8]奥泽纳姆 (J. Ozanam, 1640—1717, 法国数学家、科学院院士, 著述颇丰, 包括新的三角函数和对数表; 曾因数论方面的贡献获莱布尼茨奖. —— 译注) 的确在他 1702 年的《代数新原理 (*Nouveax élémemts d'algebre*)》中叙述了一个与布龙克尔的完全相同的证明, 其中还以 $N = 23$ 和 $N = 19$ 作为范例进行了解释; 他把它归到了费马的名下. 难道他比我们知道了更多的东西, 还是他只不过错误地理解了《*Commercium Epistolicum*》?

的, 故而将此过程反过来推, 便得到了原来问题的一个解. 这恰恰是印度数学家的 *kuṭṭaka*(粉碎机) 方法 (参看第一章 §4 和 §9); 如在第一章曾指出过, 它本质上说与求两个整数的最大公约数的欧几里得算法没有什么差别, 也与对 a/b 的连分式计算没有多少差别. 现代的读者也会注意到巴歇解法的第一步可以写成

$$\begin{pmatrix} a & b \\ x & y \end{pmatrix} = \begin{pmatrix} b & c \\ y & z \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^m,$$

使得整个过程等于是将左边的矩阵写成熟知的群 $GL(2,\mathbb{Z})$ 生成元的乘积.

解费马问题的布龙克尔方法依照了同一模式. 设 N 为非平方的正整数; 假定方程 $U^2 - NX^2 = \pm 1$ 有一个解 (u, x). 设 n 是一个满足 $n^2 < N < (n+1)^2$ 的整数; 这给出了 $u > nx$, 故而可令 $u = nx + y$, 其中 $y > 0$. 同时令 $A = N - n^2$, $B = n$, $C = 1$. 于是, (x, y) 是方程

$$(10) \qquad AX^2 - 2BXY - CY^2 = \mp 1$$

的一个解, 其中 A, B, C 为正整数使得 $B^2 + AC = N$. 现在这可逐次地变换到具有相同形状且具有越来越小的解的方程, 导向了 (恰似巴歇方法那样) 原来问题的解.

布龙克尔的方法是写出 $x = my + z$, 其中 m 是小于方程 $At^2 - 2Bt - C = 0$ 那个正根的最大整数; 他似乎暗中假定了, 对于这样选取的 m, z 必定 > 0 且 $< y$. 于是 (y, z) 是一个类似于 (10) 的方程的解, 而且这个方法可以继续下去直到找到了一个具显然解 $(u, 1)$ 的方程为止; 由于它出现在了沃利斯和布龙克尔用来测试他们方法的所有数值的情形, 包括那些费马特别提到的情形, 所以他们认为没有需要来进一步深入发掘. 费马却要了解得更好些.

为了填补以上处理方法的空隙, 有必要指出 (10) 的一个特别性质, 即那个使得布龙克尔方法得以成功应用的特性. 为简明起见, 我们要采用一个修改了的高斯记号: 记 (A, B, C) 为 (10) 左端的二次型, 这里的 A, B, C 理解为非 0 正整数; 另外, 我们对于高斯的用法也有一点改动: 如果 $At^2 - 2Bt - C$ 的正根 > 1 且其负根 > -1, 我们则说 (A, B, C) 是简约的(reduced); 出现这种情形的充要条件是 $|A - C| < 2B$, 从而 (C, B, A) 也是简约的. 对于 $A = N - n^2$, $B = n$, $C = 1$, (A, B, C) 显然是简约的. 现在, 对于任意简约形式 $F = (A, B, C)$ 让 m 还是为小于 $At^2 - 2Bt - C$ 的正根最大整数. 如果我们令

$$A' = -(Am^2 - 2Bm - C), \quad B' = Am - B, \quad C' = A,$$

则 m 便是使 $A' > 0$ 的最大整数; 于是容易看出 $B' > 0$, 以及 $F' = (A', B', C')$ 又是简约的, 还有变换

$$X = mX' + Y', \quad Y = X'$$

将 F 变成 $-F'$. 如果 $N = B^2 + AC$ 是 F 的 "行列式", 那么 F' 自然具有同一个行列式. 由于最多只有有限个具给定行列式 N 的形式 (A, B, C), 从而知道由布龙克尔方法逐次得到的二次型 F, F', 等等必定最终自身重复出现. 只要沃利斯和布龙克尔将它们的数值例子的处理稍稍比他们所做过的向前推进一点, 那么他们就必定会注意到此.

记号如上, 我们称 $F' = (A', B', C')$ 是由 $F = (A, B, C)$ 导出的形式. 随便举一个例子立刻就可表明, 形式 (C, B, A) 是由 (C', B', A') 导出的形式; 事实上我们有

$$C = (C'm^2 - 2B'm - A'), \quad B = C'm - B', \quad A = C',$$

并且 m 是使得 $C'm^2 - 2B'm - A' < 0$ 的最大整数. 现在从任意一个给定的简约形式 $F_0 = (A_0, B_0, C_0)$ 出发, 用布龙克尔过程我们得到序列 $F_1 = F_0', F_2 = F_1'$, 等等, 其中对每个 i 形式 $F_i = (A_i, B_i, C_i)$ 是由 F_{i-1} 导出的; 在一种显见的意义下, 我们可以说 F_i 是 F_0 的第 i 导出形式. 所有这些都是具行列式 N 的简约形式; 我们已经看到, 它们必定会自身重复, 故而对某个 $i \geq 0$ 和某个 $p \geq 1$ 我们有 $F_{i+p} = F_i$. 对于每个 i 令 $G_i = (C_i, B_i, A_i)$; 于是 G_0 是 G_i 的第 i 导出形式, 而 G_p 是 G_{i+p} 的第 i 导出形式. 由于 $F_{i+p} = F_i$, 故有 $G_{i+p} = G_i$, 从而 $G_p = G_0$, $F_p = F_0$; 那么对所有的 k, 我们便有 $F_{kp} = F_0$. 因而我们证明了布龙克尔的过程最终导致了初始形式 F_0 的重复, 从而导致了从那时起的一个周期序列; 如果起点是布龙克尔的, 即形式 $(N - n^2, n, 1)$, 我们必定对某个 p 有 $C_p = 1$, 因而 $A_{p-1} = 1$. 因此, 方程 $F_{p-1} = 1$ 具有平凡解 $(1, 0)$, 由此, 沿该过程的反方向倒回便得到了原问题的一个解. 由于在逐次方程 $F_i(X, Y) = \pm 1$ 中符号从一个方程到下一个交替变化, 那么如果最初是从 $U^2 - NX^2 = \pm 1$ 开始的, 它的符号则是 $\pm(-1)^{i+1}$. 因此, $F_{p-1} = 1$ 的解 $(1, 0)$ 当 p 为偶数时给出了方程 $U^2 - NX^2 = +1$ 的一个解 (u, x), 而 p 为奇数时则是 $U^2 - NX^2 = -1$ 的解. 在此时, 为了给出 $U^2 - NX^2 = +1$ 的一个解, 则不得不通过该过程到达 F_{2p}, 或者更直接地 (事实上是等价地) 将基本恒等式 (5) 应用到 $A = -N, x = z, y = t$ 的情形. 事实上, 我们在第一章已经看到过, 印度数学家是如何使用恒等式 (5) (所谓的*bhāvanā*("复合"法则)), 当一旦找到 $U^2 - NX^2 = -1$, ± 2, ± 4 的一个解时, 在 *cakravāla* 过程中找出捷径的. 沃利斯和布龙克尔也发现了只要找到一个形式 F_i, 其中 $A_i = 2$ 或 4, 则通过这个过程就可以应用完全同样的捷径到布龙克尔的方法上. 他们也注意到通过变换 (以前面同样的记号)

$$X = (m+1)X' - Y', \; Y = X'$$

来代替以前所使用的那个时, 有时整个过程可以缩短; 用现代的术语表示, 等于是说建立了 $\sqrt{N}$ 的一个所谓的 "半正则" 连分式来替代一个 "正则" 的; 在第

一章 §9 所叙述的*cakravāla* 法中, 它或多或少地对应于那个规定, 即在每一步以 $N-x^2$ 表示的整数应该使得绝对值更小而不仅是小且 >0. 如那时所指出的, 这样的捷径可以是在数值上有用的但却使得理论讨论极其麻烦.

置于上述处理方法之上的事实, 可以在应用布龙克尔过程的数值情形中十分容易地观察到. 沃利斯和布龙克尔在其中处理过 $N=13$ 的情形, 它相当典型, 后来成了在叙述他们的方法时喜欢使用的例子, 譬如, 在他 1770 年的《代数》(*Eu*.I–1,383) 中. 在 1657 年费马写给弗莱尼柯的信中提出了情形 $N=61$ 和 $N=109$, 并说 (有意误导, 或者相当恶作剧地) 他选取了十分小的数 "*pour ne vous donner pas trop de peine*"; 当然, 他必定已经知道在这两种情形中的最小解分别是

$$(1766319049, 226153980),$$

$$(158070671986249, 15140424455100),$$

而这正是选取 61 和 109 的理由.

为了证明该方法可导出全部的解, 我们还需做最后一步; 或者用现代术语表达即, 实二次域的单位群是由用上述方法得到的一个单位生成的. 为此, 只有再次 (如我们启发式地做过的, 也如沃利斯和布龙克尔所做而没有进一步向前看的) 从 $U^2-NX^2=\pm1$ 的一个解 (u,x) 出发. 它在变换 $u=nx+y$ 下变换成下一个方程 $F(x,y)=\mp1$ 的一个解 (x,y), 然后用变换 $x=mx'+y'$ 再变成再下一个方程 $F'(x',y')=\pm1$ 的一个解 (x',y'). 经验表明这导致了越来越小的整数对, 并且最终达到了 $(x,1)$ 而后则到了 $(1,0)$, 这就是该步骤的终点; 但是对此还必须知道 $0<x'<x$, $0<y'<y$ 等等才行. 对于第一步 $u=nx+y$, 条件 $u^2-Nx^2=\pm1$ 给出了

$$n^2x^2-1<u^2<(n+1)^2x^2+1;$$

这表明 $nx\le u\le(n+1)x$; 它又意味着除非 $x=1$, 否则总有 $nx<u<(n+1)x$. 至于第二及接下来的各步, 假定 (x,y) 满足

$$F(x,y)=Ax^2-2Bxy-Cy^2=\mp1.$$

令 $f(t)=F(t,1)$, $\varphi(t)=f(t)\pm y^{-2}$. 由于 f 的根位于区间 $[-1,0]$ 与 $[m,m+1]$ 之中, 我们有

$$f(-1)>0,\ f(0)<0,\ f(m)<0,\ f(m+1)>0.$$

因为这四个数均为整数, 故表明除非 $y=1$, 总有

$$\varphi(-1)>0,\ \varphi(0)<0,\ \varphi(m)<0,\ \varphi(m+1)>0.$$

由于我们对 (x, y) 的假定蕴涵了 x/y 是 φ 的根, 这便证明了 x/y 如我们所愿地落在了区间 $[m, m+1]$ 之中.

还有一个值得一提之处. 在 1654 年写给帕斯卡的关于他对 "数" 的 "发明" 的信中, 费马引述了形如 $4m+1$ 的任意素数 q 为两个平方数和的表示的一个 "普遍规则" (参看前面的 §9), 但像通常那样, 没有给出细节. 然而将布龙克尔过程用到 $N=q$, 譬如对情形 $N=13, 61, 109$ 中任一个的应用, 立刻表明一个有 $A_j=C_j$ 的形式 F_j 出现在了一个简约形式的序列中, 而该简约序列即是由这个布龙克尔过程产生的; 于是我们有 $q=B_j^2+A_j^2$. 因此, 对 $N=13$ 有 $F_2=(3,2,3)$; 对 $N=61$ 有 $F_5=(5,6,5)$; 对 $N=109$ 有 $F_7=(3,10,3)$. 这很可能就是费马的 "普遍规则" 了.

更为仔细的观察会揭示出更多的东西: 在那些情形中, 形式的序列中的周期 $(F_0, F_1, \cdots, F_{p-1})$ 有 $p=2j+1$ 个项, 其中 j 如上. 我们给出一个如下的形式证明. 设 (u, x) 为 $u^2-qx^2=1$ 的最小解; 此处的 u 必为奇数, 而 x 为偶数, 故可写出

$$\frac{u+1}{2}\cdot\frac{u-1}{2}=q\left(\frac{x}{2}\right)^2.$$

左端中的因子互素, 这是因为它们之间的差为 1, 从而 q 必定除尽其中的一个; 因此它们中的一个必具形式 v^2, 而另一个的形式为 qt^2, 从而有 $v^2-qt^2=\pm1$. 这里的符号不能为 $+$, 否则 (u, x) 不再是 $u^2-qx^2=1$ 的最小解了. 于是给出了 $v^2-qt^2=-1$. 如我们前面所见, 这意味着周期 $(F_0, F_1, \cdots, F_{p-1})$ 的项数 p 为奇数; 令 $p=2j+1$. 于是 $F_{2j+1}=F_0$, $C_{2j+1}=1$, 从而 $A_{2j}=1$. 现在我们注意到了, 如果一个行列式为 $N=B^2+C$ 的形式 $(1, B, C)$ 是简约的, 我们则必定有 $-1<B-\sqrt{N}<0$, $B=n$, $C=N-n^2$; 特别地, 我们有 $F_{2j}=(1, n, N-n^2)$. 如前, 对所有的 i 令 $G_i=(C_i, B_i, A_i)$; 我们得到 $G_{2j}=F_0$, 正如我们已看到的, G_j 是 G_{2j} 的第 j 个导出形式, 即 F_0 的导出形式; 因此它与 F_j 相同, 从而我们有 $A_j=C_j$, 这即为所要证明的.

一般说来, 假定这就是费马在给帕斯卡和惠更斯的信中谈及他的证明时心中所想到的, 这似乎也不无道理; 到底其中有多少是费马弄清楚了的必定还是个尚待考证的问题. 或许他的最严重的障碍之一是缺乏下标记号; 这在后来由莱布尼茨引进, 但仍不完善; 直到很后的下个世纪它的使用才得以普及. 面对着困难而复杂的证明, 费马会相当满足于对一些典型数值情形进行的仔细分析, 同时说服自己相信所涉及的步骤具有普遍的效力. 实际上他从未成功地写下过他的证明. 他们诸如费马自己, 像在对沃利斯的批评 (参看 §3) 中所坚持的那样, 是为了建立 "一门新的科学分支的基础" 吗? 这是我们永远也不知道的了.

§2.14 二次不定方程

现在来讨论 §11 的 (v). 恰如在考察形式 X^2+AY^2, $A=1,2,3$ 时以欧拉作为我们的向导, 而在讨论 "佩尔方程" 中以沃利斯和布龙克尔为向导那样, 在这里我们将谋取拉格朗日的帮助 (*Lag*.II,390–399).

我们从方程 $ax^2+by^2+cz^2=0$ 在有理数中求解问题开始; 假定 a,b,c 不具有相同的符号. 乘以 c 并以 z/c 替代 z, 则可重写该方程为 $z^2=Ax^2+By^2$, 其中 A 和 B 不全为负; 可假定它们均无平方因子, 否则, 譬如如果 A 有一个因子 $m^2>1$, 我们就可将 x 换作 x/m. 我们还选记号使得 $|A|\le|B|$. 当然只要找整数解就够了; 事实上, 我们可以要求 x, y, z 两两互素; 因为, 譬如如果 x 和 z 有公因子 $d>1$, 则 d^2 除尽 z^2, Ax^2, 从而除尽 By^2; 由于 B 不含平方因子, 故 d 必除尽 y, 从而可置换 x,y,z 为 $x/d,y/d,z/d$.

由于 x 和 B 的任意公因子必定除尽 z, x 必定与 B 互素, 所以它具有一个模 $|B|$ 逆 x'. 因 $Ax^2\equiv z^2 \pmod{|B|}$, 我们有 $A\equiv(x'z)^2 \pmod{|B|}$. 这表明所给方程除非 A 是模 $|B|$ 的二次剩余 (A 不必与 B 互素), 否则它可以没有解; 如果基于二次互反律的这个更加精细的方法不用的话, 那么情形究竟如何则可以通过反复试验来确定.

现假定 A 为这样的数; 令 $A\equiv a^2 \pmod{|B|}$. 再将 a 换成 a 除以 $|B|$ 的余数 r 与 $|B|-r$ 中较小的一个, 我们则可假设 $0\le a\le\frac{1}{2}|B|$. 因 A 不含平方因子, 除了 $a=\pm1$, $A=1$, 我们有 $A\ne a^2$. 将此平凡情形舍去, 我们则可记 $a^2-A=BB_1d^2$, 其中的 d 取成使得 B_1 不含平方因子. 我们有

$$|B_1|\le\left|\frac{a^2-A}{B}\right|\le\frac{1}{4}|B|+1$$

因而 $|B_1|<|B|$, 但除去在平凡情形 $B=\pm1$, $A=\pm1$ 外. 另一方面, 本章 §12 的基本恒等式 (5) 给出了

$$B_1(Bdy)^2=(a^2-A)(z^2-Ax^2)=(az\pm Ax)^2-A(ax\pm z)^2.$$

如果令 $X=ax\pm z$, $Y=Bdy$, $Z=az\pm Ax$, 这表明 (X,Y,Z) 是 $Z^2=AX^2+B_1Y^2$ 的一个解.

由于 $A\equiv a^2 \pmod{|B_1|}$, 于是这个步骤现在可以重复下去, 直到我们到达形如 $Z^2=AX^2+B_nY^2$, $|B_n|<|A|$. 我们于是可以令 $A'=B_n$, $B'=A$; 为了进一步进行下去, A' 必须是一个模 B' 的二次剩余. 依此方式继续下降, 不断地减小系数 A 和 B 的值, 我们必定要么得到了形如 $Z^2=MX^2+NY^2$ 的方程, 其中的 M 不是一个模 $|N|$ 的二次剩余, 在此情形下, 原来的方程自身不存在解,

要么得到了一个形如 $Z^2 = X^2 + NY^2$ 的方程, 它具有显然的解 $(1,0,1)$; 在后面这种情形, 以此过程的反推便得到了原方程的一个解.

显而易见, 这是个典型的 "下降法", 与费马的一般原理十分一致; 事实上, 其基本思想相当接近于在 §13 中为处理佩尔方程所叙述的那些思想 (或许更像是在第一章 §9 中叙述的印度人的方法). 除了费马说他已经解决了这个问题的陈述外, 也除了他的方法十分符合我们所了解的事实外. 这里又一次没有证据能使我们相信费马是按照上述方式进行处理的.

如果我们试图处理他关于每个数是 "三个三角数、四个平方数、五个五角数, 等等" 之和的著名陈述 (参看前面的 §5 及 §9(i)), 我们便处在了一个十分糟糕的地位. 早在 1638 年这个陈述就出现了 (*Fe*.II,65), 这似乎是他最不可能对其有任何一种证明的时候了. 1654 年写信给帕斯卡时, 他把它提成是迄今为止他的最重要的结果 (*Fe*.II,313), 另外只是补充说, 其证明有赖于他的关于两个平方数和的定理. 在他的《丢番图》中 (*Fe*.I,305, Obs.XVIII), 他写道 "它依赖于 (数论中) 最深刻的秘密", 他计划写一整本书全力来解说它. 在 1659 年写给惠更斯的信 (*Fe*.II,433) 中他仅仅复述了关于四个平方数的和的断言, 而略去了他较早陈述的其他部分; 这个省略应该被赋予了什么意义吗? 这次他补充说, 其证明在于指出 "如果某个数不是这种类型的" (即不是不超过四个平方数的和), "就会有一个更小数据有这同样的性质, 等等". 我们的确知道有这一类型的证明 (参看第三章 §9); 它们或多或少类似于对于两个平方数和的相应证明, 但是它们事先假定了关于四个平方数的和的乘积的欧拉恒等式, 而此等式不是那么轻易能发现的; 可以确信在费马的著述中并没有它的痕迹.

至于 "三角数" 与三个平方数的和, 问题甚至更加神秘. 每个整数是三个 "三角数" 的和等于是说每个形如 $8n+3$ 的整数是三个平方数之和; 由此, 如勒让德在他的《数论 (*Théorie de Nombres*)》中所指出的 (3e éd.t.,II,pp.331–356), 我们可以推导出 (并不十分容易, 但至少是初等的) 费马关于 "四个平方数, 五个五角数, 等等" 的更进一步的断言. 三个平方数的和也在他的《丢番图》的边白注记中提到 (*Fe*.I,314–315,Obs.XXVII); 这里的《丢番图》提出的问题是, 是否一个整数 $N = 3n+1$ 是三个平方数的和 (整数的或是分数的); 为了达到这点, 费马说, 它必须 (且隐含着充分的) 不满足下面的任何一个同余式:

$$n \equiv (1+4+4^2+\cdots+4^{r-1}) + 2\times 4^r \pmod{8\times 4^r}.$$

这个注记具有属于费马事业早期的所有形态. 他的条件等于是说数 $N = 3n+1$ 必不具有形式 $4^r(8m+7)$, 它的确就是 N 为三个平方数之和的条件; 费马关于这个事实的知识只能是基于 "归纳法" 得到的, 这是因为迟至 1658 年他还不能证明如果 p 是个形如 $8n-1$ 的素数, 则 $2p$ 是三个平方数之和; 后面这

件事在他最后给沃利斯的信 (*Fe*.II,405) 中说成是 "在科农意义下是正确的 (true in the sense of Conon)", 即只是猜想而仍未证明的意思*24. 对我们来说, 前面提到的对于《丢番图》的考察的首要兴趣在于它实质上给出了 2- 进位展开

$$\frac{-1}{3} = \frac{1}{1-4} = 1 + 4 + 4^2 + \cdots + 4^r \pmod{4^r}.$$

然而, 对于 "三个三角数之和", 只要没有出现看起来归属于费马的证明, 这个秘密就仍在继续.

§2.15 对亏格 1 的方程的追本溯源

如果认真读取费马在 1659 年给惠更斯信中的话, 人们必定会得出结论说, 他在其职业生涯的相对晚期从事了对诸如 $x^3+y^3=z^3$, $x^2+2=y^3$, $x^2+4=y^3$ 此类丢番图方程的研究. 然而这些方程中的第一个已在 1638 年给梅森的信中就出现过 (*Fe*.II,65), 而且在 1640 年还连同几个同一类型的方程再次出现 (*Fe*.II,195), 并明显地暗示说, 这些方程除了那些显然解外没有其他解. 在 1659 年他的记忆或许已经出了毛病; 更可能的是, 甚至在 1640 年, 他也只是希望提到他对这些方程取得了一个相当满意论证的时间, 而不是那些仅仅建立在似是而非论证基础上的猜测. 确实, 他对于亏格 1 的丢番图方程进行密集研究的时期是从 1641 年左右开始的, 这正值弗莱尼柯向他提出有关毕达哥拉斯三角形的问题的时刻 (他曾说过, "因对它的爱" 他研究了 "数"; 参看 *Fe*.II,241,244,265); 当然他们两个人对他们的《丢番图》必定是读读停停. 最终从迪格比那里得知 (*Fe*.II,362), 弗莱尼柯对这些东西的兴趣减退了; 幸运的是, 费马的兴趣并未减少, 至少他的教会信友比利, 以富于技巧的提问并配以溢美之词, 成功地拽住了费马足够长的时间以从他那里获取资料, 后来这些资料成了比利的《*Inventum Novum*》(参看前面的 §1).

我们在第一章 §10 已看到, 在《丢番图》中最重要的问题都与亏格 0 和 1 的曲线有关. 对于费马而言这种曲线几乎变成了他的唯一专注. 仅仅在一个令人不快的场合费马提到过一条具更高亏格的曲线, 而且几乎没有任何怀疑, 这只不过是他的一个误解罢了, 即便如此, 命运的无常总使人意外, 在无知者的眼里他的声誉竟主要表现在它上面. 我们对此当然指的是在他的通常被称作 "费马大定理" 的陈述中那个不慎用词 "*et generaliter nullam in infinitum potestatem*"*25.

*24Conon, 686—687 年时的教皇, 当选时就已衰老, 11 个月后死亡, 故有此一说.

*25这是 "费马大定理" 陈述的拉丁文中第三句的一段; 原文为 "*Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet*".

这个陈述即“没有一个立方数能分解成两个立方数, 没有一个四次方数能分解为两个四次方数, 并且一般地, 没有一个高于二次的方幂能分解为两个同类型的数”, 这是他写在他的《丢番图》的较前章节的边白上的 (*Fe*.I,291,Obs.II), 并补充写道, 他已经发现了对此的一个非凡的证明“而由于边白太窄写不下它”. 他怎么能猜到他在写一个不朽名句呢? 我们知道他有对于四次情形的证明 (参看前面 §10); 他也可能已构想好了对于三次情形的证明, 这个证明或许就类似于欧拉在 1753 年发现的那个吧 (参看下文的 §16); 他时常重复前面的那两个陈述 (譬如 *Fe*.II,65,376,433), 而再也不提那个一般性的陈述了. 或者仅仅一个短暂的时刻, 或者在他更年轻的时候 (参看前面的 §3), 他必定使自己迷惑过, 以为他已经有了一个一般性证明的原理; 在那些日子里, 他心里想了些什么永不会为人所知了.

另一方面, 我们所拥有的他论述亏格 1 曲线的方法是条理非常分明的; 它仍然是这类曲线的现代理论基础. 它被自然地分为两部分; 第一部分直接由丢番图那里的启示而来, 为方便起见, 相对于“下降法”我们不妨称这部分为提升法 (ascent), 而下降法正可看成是更具费马自己特点的. 尽管对于下降法的一般特性没有什么可怀疑的, 但对于下降法的信息较之于费马关于提升法的陈述 (譬如, *Fe*.I,291–292,Obs.III; *Fe*.I,297–299,Obs.VIII–IX; *Fe*.I,322–325,Obs.XXX;*Fe*.I,328–329,Obs.XXXIV; *Fe*.I,334–339,Obs.XLIII-XLIV) 以及比利在他的《*Inventum Novum*》中所收集的丰富 (真的是超级多的) 资料 (=*Fe*.III,325–398) 来说却相当不足.

用现代术语来说,“提升法”只不过是从亏格 1 的曲线方程的几个“可见”的解推导出新解的方法, 在大多数情形中会有无限多个解. 这里的新东西当然不是该方法的原理; 它已被丢番图系统地应用过, 并且费马 (索引同上) 和比利都同样把它指认为“*methodus vulgaris*”, 即传统方法 (也可参看巴歇对 *Dioph*.VI,24_b 的冗长评注). 新颖之处在于费马对它做出的极其广泛的运用, 给了他至少相当于我们系统使用标准三次曲线上有理点的群论性质所得到的东西 (参看下文的附录 III). 显然费马为此十分自豪; 在他的《丢番图》(*Fe*.I,334,Obs.XLIII) 边白上为自己写下了一些话, 他称它为“*nostra inventio* (我们的创造)”, 并且有一次写给比利说:“它使得最大的专家们大吃一惊”[“*C'est une de mes inventions qui a quelquesfois estonné les plus grands maistres, et particulierement Monsieur Frenicle...*”; *Fe*.II,437]. 档案材料表明费马用此方法处理了下面一些类型的问题, 其中大多数出现在《丢番图》中:

(I)“二重方程”, 其形如

$$Ax^2+Bx+C=u^2,\quad A'x^2+B'x+C'=v^2,$$

并假定或者 A 和 A', 或者 C 和 C' 为平方数; 可设左端在射影直线上没有公共零点, 这是因为不然的话它就定义了一条亏格为 0 的曲线 (对此可参看前面的 §14). 对我们的目的来说, 我们把该曲线看作是嵌入在射影空间中的, 其齐次坐标为 $(1, x, u, v)$. 如果 $A = a^2$, $A' = a'^2$, 我们则在无穷远有四个有理点

$$P_{\pm,\pm} = (0, 1, \pm a, \pm a').$$

类似地, 如果 $C = c^2$, $C' = c'^2$, 我们则有四个 "平凡" 解

$$Q_{\pm,\pm} = (1, 0, \pm c, \pm c').$$

当然, 在费马的眼里, 正如同在丢番图的眼里一样, 这些不是 "解". 从丢番图那里继承下来的传统方法 (参看第一章 §10) 譬如在 $A = a^2$, $A' = a'^2$ 的情形可写成

$$(a'u + av)(a'u - av) = B''x + C'',$$

其中 $B'' = A'B - AB'$, $C'' = A'C - AC'$, 于是

$$a'u + av = t, \quad a'u - av = \frac{1}{t}(B''x + C''),$$

$$u = \frac{1}{2a'}\left(t + \frac{B''x + C''}{t}\right).$$

将后面这个 u 的值带入所给的方程中的第一个, 并取 $t = \pm t_0$, $t_0 = B''/2aa'$, 我们便得到了 x 的一个线性方程, 从而得到了一个解. 我们现在用现代术语来阐明: 在所给曲线上考虑函数

$$f = a'u + av - t_0;$$

容易看出它在 P_{++} 和 P_{--} 有一个单极点, 在 P_{-+} 无极点, 而在 P_{+-} 有一个零点; 换句话说, 我们已经构造了由等价关系 $M \sim P_{++} + P_{--} - P_{+-}$ 给出的点 (参看附录 II). 在情形 $C = c^2$, $C' = c'^2$, 自然有相似的构造. 如果所有的 A, A', C, C' 均为平方数, 费马有个额外的构造, 它基于 (以现代术语表示) 函数 $a'(u \pm c) \pm a(v \pm c')$, 此函数产生了等价于 $P_{++} + P_{--} - Q_{++}$ 的点, 等等.

现在, 在不管用这些方法中哪一个得到一个有理点 $M = (x_0, u_0, v_0)$ 之后, 费马用 $x + x_0$ 替换 x 得到新的一对方程, 它们中的常数项为平方数, 在此之后这个过程又可以重新开始, 并无限定地继续下去; 他说只是 "他的发明". 当然这不能使他避免一些特殊情形, 那时该过程会反复地导向同一个解; 这对应了该过程的起点在解群中具有有限阶. 但通常他会毫不犹豫地断言他将得到无限多个解 (参看, 譬如 *Fe.*II,248–249,259–260,263), 而他总是对的.

(II) 其次考虑方程

$$Ax^4+Bx^3+Cx^2+Dx+E=y^2;$$

以现代术语表达, 我们可将它看为定义了射影直线的一个二重覆叠; 当然我们假定方程左端没有重根, 并且 A 或 E 为平方数. 如果 $A=a^2$, 则在无穷远有两个有理点 P_+ 和 P_-, 分别由展开式

$$y=\pm(ax^2+bx+c+\cdots)$$

给出, 其中 $b=B/2a$, $c=(4AC-B^2)/8Aa$. 于是 "*methodus vulgaris*" 便是在所给方程中将 y 代入值 $y=ax^2+bx+c$, 它导出了一个 x 的线性方程. 用附录 II 中所解释的语言表达, 这等于是考虑了函数 $y-ax^2-bx-c$, 而它在 P_- 有一个二重极点, 而在 P_+ 有个零点; 他的余下的零点于是为 $M\sim 2P_--P_+$. 相似地, 如果 $E=e^2$, 我们有两个点 $Q_\pm=(0,\pm e)$; 令 $y=a'x^2+b'x+e$, 其中 a', b' 为两个适当的数, 于是得到点 $M'\sim 2Q_--Q_+$. 如果我们全有 $A=a^2$ 和 $E=e^2$, 则依照费马, 可以有变换 $y=\pm ax^2+mx\pm e$, 其中 m 选取得使按此方式得到的方程, 在除以 x 的一个幂后成为对 x 是线性的. 这导出了点 $\sim 2P_\pm-Q_\pm$, $2Q_\pm-P_\pm$. 这个步骤于是可以像前面 (I) 中那样, 在找到一个解 (x_0,y_0) 后, 以 $x+x_0$ 替换 x 进行迭代.

(III) 相似的方法可以应用到方程

$$Ax^3+Bx^2+Cx+D=y^2$$

上, 其中假定了 $D=d^2$, 或者应用到方程

$$Ax^3+Bx^2+Cx+D=y^3,$$

其中或 A 或 D 为立方数. 在这些情形的方法等价于那个熟知的, 一条三次曲线与在该曲线上一个有理点的切线的相交. 费马留意到这个几何解释了吗? 在他对解析几何的研究中, 他涉及构建由方程给出的平面曲线的切线问题, 并且特别处理了 "半三次抛物线" $ay^2=x^3$, "蔓叶线" $x(x^2+y^2)=ay^2$, 以及 "蚌线" $(x^2+y^2)(y-a)^2=b^2y^2$ (参看 *Fe*.I,159–161 和 218). 由于缺少证据, 这个令人着迷的问题仍然没有答案.

另一方面, 值得注意的是, 似乎费马没有关于一条三次曲线与通过事先已知的两个有理点的直线相交的简单想法, 不管是在几何的还是在代数的外衣下都没有. 但在牛顿的一些手稿中人们发现了这个思想 (*New*.IV,112–114), 这明显是首次, 并且是以完整叙述的形式出现的; 推测起来, 大概写在塞缪尔 · 费马 1670

年的《丢番图》(即包含了比利的《*Inventum Novum*》的那一卷) 出现后不久, 可能受到了该书出版的激励吧.

(IV) 下面的问题只是 (I) 的一个变形, 用一个简单的变量变换就可把它变换到 (I), 如果不是费马似乎对论述它的方式颇感自豪 (参看 *Fe.*I,334,Obs.XLIII, 以及 *Inv.Nov.*II,1=*Fe.*III,360) 的话, 几乎不值得单独提到它. 它由 "三重方程"

$$Ax+B=u^2,\ A'x+B'=v^2,\ A''x+B''=w^2$$

构成, 其中 B, B', B'' 为平方数; 在以 $(1,u,v,w)$ 为坐标的射影空间中, 它定义了一个空间四次曲线, 并有 8 个 "可见" 有理点. 如果 $B=b^2$, 则令 $x=2bt+At^2$, $u=b+At$, 于是得到了一个 "二重方程", 对于它, 根据前面所解释过的方案, 必须使用这些有理点.

我们注意到所有这些中并没有什么数论, 每一步在任意域上都有效, 特别是在实数域上. 在费马的眼里这样的工作因而应划归于 "几何"; 我们宁愿把它描述为代数几何, 这就像丢番图的工作那样, 还有韦达的工作, 代数几何可看做它的推广; 对此可参看第一章的 §10, 以及在那里的从费马在 1657 年对英国数学家的挑战中引述的他的评述 (*Fe.*II,335). 在处理这些问题时, 费马有两个动机.

首先, 尽管丢番图通常对任何给出的问题只要能有一个解就满足了, 但有时他也会要求更多的解; 例如在 *Dioph.*V,8_b 中, 他给出了一个求三个面积相等的毕达哥拉斯三角形的方案, 而韦达则在他的《*Zetetica*》(*Zet.*IV,11=Op.p.70–71) 中将其翻译成了代数语言. 如果将此三角形在差一个因子的范围内取作 $(2pq, p^2-q^2, p^2+q^2)$, 然后令 $x=q/p$ 或 $x=p/q$, 记 A 为其面积, 于是问题等于是找一条具有三个有理点的曲线 $|x-x^3|=Ay^2$. 丢番图的方法是找出 $x-x^3=x'-x'^3$, 即 $x^2+xx'+x'^2=1$ 的一个解, 因此这提供了两个面积为 $A=x^3-x$ 的三角形, 然后注意到 $x+x'$ 是 $A=X^3-X$ 的一个解; 我们对此的解释是说, 因为 $(x,1)$ 和 $(x',1)$ 位于三次曲线 $AY^2=X-X^3$ 上, 故该三次曲线与直线 $Y=1$ 的第三个交点 $(-x-x',1)$ 也必定是有理的; 但是, 这并不表示丢番图、韦达, 甚至费马从中看出了这是一个暗含着的一般原理的应用. 与丢番图和韦达不同, 费马只是从一个毕达哥拉斯三角形开始的, 如此得到了一条具一个已知有理点的曲线 $x-x^3=Ay^2$, 然后用在那个点上的切线与此三次曲线交, 并按需要重复这个步骤; 这至少被他描述为他的基本方法, 然而 (并不令人吃惊地) 他也有多种方法来将这同一个问题化到一个 "二重方程", 然后将在 (I) 中所叙述的方法应用于它 (参看 *Fe.*I,309–311,Obs.XXIII, 以及 *Inv,Nov.*I,38=*Fe.*III,348).

为什么费马对传统方法不满意, 还有另外的原因; 这就是 "*methodus vulgaris*" 常常导致负数的解; 在传统的观点看来这简直就是无解. 举将两个给定立方数的和或差表达为另外两个立方数的和或差的问题为例 (显然是由丢番图

在他的失散了的《*Porisms*》中提出的或者解决了的; 参看 *Dioph.*V,16); 韦达在他的《*Zetetica*》论述过它 (*Zet.*IV,18–20=Op.74–75); 巴歇在他对 *Dioph.*IV,2 的评注中复制了韦达的论述, 包括他的数值例子 (而没有任何鸣谢之词; 参看第一章 §12). 问题当然在于从一条曲线 $X^3+Y^3=A$ 上的一个有理点 (a,b) 推导出第二个有理点, 而不同的是, 韦达和巴歇还按 a, b, x, y 的符号将它分成了各种情形.

韦达, 还有追随他的巴歇, 对此满足于 "*methodus vulgaris*"; 实际上, 他们用曲线在其 (a,b) 的切线与该曲线相交; 这给出了解

$$x=a\cdot\frac{a^3+2b^3}{a^3-b^3},\quad y=b\cdot\frac{2a^3+b^3}{b^3-a^3},$$

依照他们的观点看, 当 a, b 具有指定的符号时, 只有当 x, y 也具有指定的符号这才算满意. 举例来说, 如果问题是求两个立方数使得他们的和为两个已知的立方数 p^3 和 q^3 的差, 那么在我们目前使用的记号下, 就可取 $a=p$, $b=-q$, $p>q$, 并要求 x, y 为正, 故而韦达的公式当 $p^3>2q^3$ 时解决了这个问题, 但对其余的情形则没能解决. 如费马所指出的, 他们从来也没能解决求两个立方数使得它们的和为两个已知立方数之和的问题. 费马对于这样一批问题的方案 (*Fe.*I,291–292,Obs.III;I,297–299,Obs.VIII–IX) 是将韦达的方法反复迭代多次, 直到得到所需的一个解为止, 然后如果还想要更多的解则再按需进行多次迭代.[9] 在这里他也没有给出对于这个总能成功进行的事实给出正式的证明, 似乎已满足于他对这些事物的经验了.

至于对 "提升法" 的第一次发现, 我们有费马在 1644 年给卡尔卡维的信中的陈述为证, 在那里他提到弗莱尼柯有一次 ("*auterfois*") 向他提出的下面的关于毕达哥拉斯三角形 (即整数三元组 a,b,c 使得 $a^2+b^2=c^2$) 的问题 (参看弗莱尼柯 1641 年给费马的信, *Fe.*II,241), 这是个曾使得他们两人着迷的问题; 他对卡尔卡维写道, "*je ne voyois pas même de voye pour y venir* ("我甚至不知道有什么办法来对付它"); 但是到了 1644 年那个时候他便能解决它们了 (*Fe.*II,265):

(A) 求一三角形使得 $a>b$, 且 $(a-b)^2-2b^2$ 是个平方数;

(B) 求一三角形使得 c 和 $a+b$ 为平方数.

如弗莱尼柯所指出, 这两个问题紧密相关. 要看出这点, 在 (A) 中令 $x=a/b$, 并看到该问题等价于 "二重方程"

$$(11)\qquad x^2+1=u^2,\quad x^2-2x-1=v^2$$

[9] 按推测, 费马并不知道同一想法已经为 Albert Girard (1595—1632, 生于法国的荷兰数学家, 其兴趣在代数、三角学 (首先引进 sin, tan 等记号) 及数论. —— 译注) 所知, 这是在他翻译丢番图的 "书" V 和 VI 时了解到的; 参看《*Les Œuvres Matematiques de Simon Stevin...reveu, corrigé et augmenté par Albert Girard*》, Leyde, Elservier 1634, pp. 159–160.

在 $x>1$ 的条件下求有理数解. 至于 (B), 令 d 为 a,b,c 的 g.c.d., 并记 (参看第一章 §5):

$$(12)\qquad a'=\frac{a}{d}=2pq,\ b'=\frac{b}{d}=p^2-q^2,\ c'=\frac{c}{d}=p^2+q^2,$$

其中 p 与 q 互素, $p>q$, 并且 $p-q$ 为奇数. 令 δ 为 c' 与 $a'+b'$ 的 g.c.d.; δ 除尽 $a'+b'\pm c'$, 即 $2p(p+q)$ 及 $2q(p-q)$, 它们的 g.c.d.为 2; 因为 c' 为奇数, δ 为 1, 故 d 是 c 和 $a+b$ 的 g.c.d. 现在, 如果 c 和 $a+b$ 为平方数, d 也必定是个平方数, 从而 c' 和 $a'+b'$ 也是; 又, 如果 p 与 q 互素则除了 $p-q$ 为奇数外, p^2+q^2 不是一个平方数. 令 $x=-p/q$, 我们发现 (B) 也等价于二重方程 (11), 但是边条件为 $x<-1$.

这些问题以及同样类型的其他问题, 在 1643 年与 1644 年费马的通信中反复出现; 显然这正是在这类问题上他取得突破的年代. 在 1644 年他寄给了卡尔卡维他对于 (A) 的解 $(1517,156,1525)$. 1643 年他寄给梅森他对 (B) 的解

$$a=4565486027761,\ b=1061652293520,\ c=4687298610289$$

(*Fe*.II,261; 参看 *Fe*.II,259–260,263); 这对应于 (12) 中的 $p=2150905$, $q=246792$. 问题 (A) 和 (B) 是他在他的《丢番图》边白上作为显示他的迭代法的例子 (*Fe*.I,336–338,Obs.XLIV), 他形容它们为 "非常困难的问题", 除此以外不能有其他的解法; 他解 (B) 过程的细节可在《*Iventum Novum*》中找到 (*Inv.Nov*.I,22,25,45,III,32=*Fe*.III,338,340–341,353–354,388,389); 他们中的一个应该能看出, 该问题同于使得 $c(a+b)$ 为平方数的问题 (因为如上所示, 可以假定 $a+b$ 与 c 互素); 那么, 若令 $z=p/q$, 则必须使得 $(z^2+1)(z^2+2z-1)$ 为一平方数, 而此可通过反复应用在前面 (II) 中费马的方法之一来完成 (*Inv.Nov*. III,32=Fe.III,388–389). 另外, 在同一边白注记 (*Fe*. I,337) 中, 他不揣冒昧地 "充满自信地断言" 他对于 (A) 和 (B) 的解是最小的可能解; 这由拉格朗日在 1777 年证实 (参看下文的 §16, 以及附录 V).

§2.16 再论下降法

经验立即表明, 费马的迭代法迅速地导出了非常大的整数. 当人们希望的不是对所给问题的越来越多的解, 相反地, 而是希望证明没有解, 或者至少只要解存在, 则所有这些解能够用一些正规的方法从几个已知的解推导出来. 对这种典型情形的一个证明已在前面的 §10 叙述过, 在那里证明了一个毕达哥拉斯三角形不可能有一个平方数的面积; 这等价于证明 $x-x^3=y^2$ 除了 $y=0$, $x=0$ 或者 ±1 外没有其他的有理解 (参看前面 §15). 如我们曾经见过的那样, 为此需

要一个 “下降法”, 只要假定有一个解存在, 那么利用它就可以产生越来越小的解. 对此的另一个例子是由方程 $x^2 - Ny^2 = 1$ (“佩尔方程”) 给出的, 我们在前面的 §13 讨论过它; 它具有亏格 0 而非 1, 然而为了得到它的完全解也需要使用下降法.

对于这种 “负向” 的问题, 费马在其 1659 年给惠更斯的通信中引用了四个例子 (*Fe.*II,433–434). 十分奇怪的是, 这四个中的最后一个恰是他的那个对形如 $2^{2^n}+1$ 为素数的错误断言 (参看前面的 §4), 他在一年多一点以前还是非常谨慎地将其仅仅作为一个猜想提了出来 (*Fe.*II,404). 惠更斯对此表示了怀疑 (*Huy.*II,212=Fe.IV,122), 并在该信的抄写件的边白上记上了这个不同的看法 (*Huy.*II,462); 我们怀疑是否坏的健康状况暂时将费马的注意力从此处转移开了. 至于对其他三个例子, 它们的公共之处明显是其部分地依赖于费马关于二次型 $X^2 + AY^2$ 对于 $A = 1, 2, 3$ 的理论, 更特别地依赖于在前面叙述过的 §9 的引理 4 和 §12 的引理 5. 我们首先将很快论述其中的两个, 这两个已经在费马 1657 年给迪格比的信中当作了挑战问题 (*Fe.*II,345) 而且似乎它们差不多就是这两个引理的直接推论. 在其中的一个情形, 我们必须证明 $x^2 + 2 = y^3$ 除去 $(5, 3)$ 外没有其他的自然数解. 事实上, 如果 (x, y) 是一个解, 那么 §12 的引理 5 (或者另外的, $\mathbb{Z}[\sqrt{2}]$ 的初等理论, 对此可参看附录 I) 表明存在两个整数 u, v 使得 $y = u^2 + 2v^2$, $x = u^3 - 6uv^2$, $1 = 3u^2v - 2v^3$. 后面的这个公式表明 $v = \pm 1$, $3u^2 = 2 \pm 1$, 从而 $v = 1$, $u^2 = 1$, $y = 3$, $x = \pm 5$. 在另外一个情形, 我们必须解 $x^2 + 4 = y^3$. 在此应用 §9 的引理 4. 如果 x 为奇数, 我们必有 $y = u^2 + v^2$, $x = u^3 - 3uv^2$, $2 = v^3 - 3vu^2$; 因为 v 除尽 2, 它必为 ± 1 或者 ± 2; 如果它是 ± 1, 那么 x 就会是偶数; 如果 $v = \pm 2$, 则我们有 $2 = \pm(8 - 6u^2)$, 从而 $u^2 = 1$, $y = 5$, $x = 11$. 另一方面, 如果 x 为偶数, 令 $x = 2x'$, $y = 2y'$; 于是, $x'^2 + 1 = 2y'^3$, 从而 x' 必定为奇. 令 $z = (x'+1)/2$, $t = (x'-1)/2$; 因此给出了

$$z - t = 1,\ y'^3 = z^2 + t^2.$$

再应用 §9 的引理 4; 我们得到

$$z = u^2 - 3uv^2,\ t = v^3 - 3vu^2,\ 1 = z - t = (u - v)(u^2 + 4uv + v^2).$$

显然它除了 $u = 1$, $v = 0$ 以及 $u = 0$, $v = -1$ 没有其他的解, 而它们给出了 $z = 1$ 或者 0, $x' = \pm 1$, $x = \pm 2$, $y = 2$.

十分不同而且我们非常感兴趣的是求方程 $x^3 + y^3 = z^3$ 整数解的情形, 或者等价地, 求方程 $X^3 + Y^3 = 1$ 的有理数解的情形, 这是作为 1659 年寄给惠更斯四个问题中的第一个. 它可被视作在前面 §10 所讨论问题的一个伴同问题, 这二者都是属于将 “真正的” 下降法用于亏格 1 曲线的情形; 与这两个一

起的这样的问题还有在费马 1640 年给弗莱尼柯信中叙述的一个问题, 即, “求组成算术级数的四个平方数”. 在那些最初的日子里, 费马或许只不过对这些问题无解有一点似是而非的推断; 然而最终他必定也对第三个问题得到了一个正式的证明, 这是因为比利在他的书《*Inventum Novum*》中是这样告诉我们的 (*Inv.Nov.*II,11=*Fe.*III,365).

倘若比利表现出一些对这种“负向”陈述的好奇心而不是冗长地一个接一个地排列着费马的迭代法, 甚至它们中还有不少是他自己设计的东西, 还有一些甚至没有任何正面的意义, 那我们将该如何感谢这位好心的耶稣会教士啊! 因此留给我们的只有尽我们所能去重新构造费马的一些最感兴趣的使用下降法的证明, 并且再次如以前所做过的那样, 去到欧拉和拉格朗日那里寻求援手. 当如此做时, 我们不应该忘记这是在以这种证明的精神来接纳许多与其他一样出色的但可能有所变化的方法; 对此的例子充满在欧拉的著作中; 对这种现象的解释只能在亏格 1 曲线的现代算术理论中才可以找到. 无需深入细节, 只要提及这种证明总是一成不变地从一条亏格 1 曲线的方程进行到另一条的方程 (举例说, 在 §10 中具齐次形式的曲线在那里则作为 $pq(p+q)(p-q)=m^2$, $x^4-y^4=z^2$, $r^4+4s^4=x^2$, 即以非齐次的形式 $X^3-X=Y^2$, $X^4-1=Y^2$, $X^4+4=Y^2$ 出现), 并且再由此返回到原来的方程就足够了. 从一条走到下一条曲线所使用的公式有时仅仅定义了一个双有理对应, 遇到这种情形则没有取得什么真正的进展; 但在最大部分情形它们定义了在椭圆曲线的经典理论中习惯称作的“变换”(现代术语称为“同源 (Isogeny)”),且通常阶数为 2 或 3; 在特殊情形, 这样一个变换正是个复数乘法, 而它的公式, 例如, 隐含在 §10 的证明之中以及下面将要叙述的证明之中.

因为所处的境况, 任何重新构造的努力也只可能是一个碰巧遇上的命题; 所有能够做的只是显示费马得到他的结果的那种方式. 至于四个平方数组成算术级数的问题在欧拉 1780 年的一篇文章中有所论述, 该文在他死后方才发表 (*Eu.*在 E758 的 I-5,56–60); 它写得多少有点乱, 显然是由他的助手在他完全失明时写的 (参看第三章). 一个更加直接更加优美的证明可以在 J. Itard 的《*Arithmétique et Théorie des Nombres*》, P.U.F., Paris 1973,p.112 中找到. 以现代亏格 1 曲线理论的观点来寻求展示下降法机理的一个证明将在附录 IV 中给出.

现在我们转到方程 $x^3+y^3=z^3$; 它定义了射影平面中的一条亏格 1 的曲线. 除了说用下降法处理外, 费马对于该方程的处理没有留下任何明示. 是欧拉 1753 年在他写信给哥德巴赫时, 第一次提到他发现了一个证明, 这个证明与已知的对 $x^4+y^4=z^4$ 的证明如此不同, 以致它让他完全失去了将其推广为对 n 次幂情形的一般性证明的希望 (*Corr.*I,618). 他在 1760 年提到了他对三次情形的证明 (参看第三章 §14), 而后在他 1770 年的《代数》的最后一章中给出了

详尽的解释 (Eu.I-1,486), 唯一的差别是, 在 1760 年他指出它是建立在二次型 X^2+3Y^2 的理论基础上的, 而在 1770 年他利用了域 $\mathbb{Q}(\sqrt{-3})$. 如我们反复提到的 (参看附录 I), 那两种解释的模式本质上是等价的, 并可轻易地从一种翻译成另一种; 当然, 费马会使用前一种, 而我们在这里也将这样做; 不然的话, 我们就要紧紧地尾随欧拉去了.

不妨假定 x, y, z 互素; 于是他们中的一个必为偶数, 而另两个为奇数; 如有必要改变它们的符号, 于是可重写该方程为 $x^3+y^3=z^3$, 其中 z 为偶, x 和 y 为奇; 令 $x=p+q$, $y=p-q$. 我们便有 $2p(p^2+3q^2)=z^3$. 由于 $p\pm q$ 为奇数, 故 p^2+3q^2 为奇数; 由于 z 为偶数, 于是 p 必为 4 的一个倍数, 而 q 必为奇数. 将我们的方程写为

$$\frac{p}{4}(p^2+3q^2)=\left(\frac{z}{2}\right)^3,$$

现按照 z 是否为 3 的倍数分成两种情形. 如果不是, 则前面方程的两个因子互素, 故它们的每一个必定为立方数:

$$p=4r^3, \quad p^2+3q^2=s^3.$$

应用 §12 的引理 5; 这给出了

$$p=u(u+3v)(u-3v), \quad q=3v(u^2-v^2),$$

其中 u, v 必互素; 由于 q 为奇, 故 v 必为奇而 u 为偶. 因 $p=4r^3$, 这表明 $u/4$ 是个整数, 并为立方数, 另外 $u+3v$ 和 $u-3v$ 均为立方数. 现令 $u=4e^3$, $u+3v=f^3$, $u-3v=g^3$, 我们的得到了 $f^3+g^3=(2e)^3$; 这是原来方程的一个解, 显然是些更小的数.

如果 z 因而 p 为 3 的倍数, 则 q 便不是; 我们现在可写出

$$\frac{p}{4}\left[q^2+3\left(\frac{p}{3}\right)^2\right]=9\left(\frac{z}{6}\right)^3.$$

因此 $p/4$ 必为 9 的倍数, 并且 $p/36$ 和 $q^2+3(p/3)^2$ 的乘积是个立方数; 由于这两个因子互素, 它们必定各自都是平方数, 从而我们可以应用 §12 的引理 5, 并将其写成

$$p=36r^3,\ q=u(u^2-9v^2),\ \frac{p}{3}=3v(u^2-v^2),$$

因此

$$-4r^3=v(v+u)(v-u).$$

这里再次有 u 和 v 必互素, u 必为奇且 v 为偶. 于是 $2v$, $v+u$ 与 $v-u$ 必为立方数; 由于这里的第一个是后两个的和, 于是这又是原方程的一个解. 得到了越来越小的解, 正如费马所说, 这便导出了矛盾.

最后前面 §15 中所引述的关于对问题 (A) 和 (B) 数值解的“充满自信的断言”应该得到一点评述. 由于涉及大的数, 特别是 (B) 的解, 仅仅反复试验自然不可能证明这些是最小的解. 拉格朗日在 1777 年终将该事厘清 (*Lag.*IV,377–398); 再将该问题换成本质上等价的求 $2x^4-y^4=z^2$ 的整数解的问题 (参看下文的附录 V) 后, 他将费马自己的下降法应用于它来处理这个问题; 尽管原理是一样的, 但细节实质上比费马的方程 $x^4-y^4=z^2$ 要复杂了许多. 然而结论却是不同的; 不是去证明除去平凡解外不存在其他解, 而是发现所有的解, 现在均可从显然可见的解出发, 利用在附录 III 和 IV 中叙述的步骤或者 (其结果一样, 至少在当前的情形如此) 利用在前面 §15 所叙述的费马的步骤得到. 用现代语言表达, 即由 §15 的“二重方程” (11) 定义的空间四次曲线, 以及四次曲线 $2X^4-1=Z^2$ 是秩为 1 的、相互同源的曲线. 考虑由弗莱尼柯和费马以公式表示的问题 (A) 和 (B) 所蕴涵的边条件, 我们便能验证费马的解的确是最小的 (参看附录 V).

费马得到了那样一个证明吗? 这并不是绝对不可能的, 这是因为拉格朗日的方法正是属于他自己的. 然而我们宁愿想象, 他仅仅让他自己被与佩尔方程的类比所引导, 在那里解群也像这里一样, 是一个无限循环群与一个二阶群的乘积; 在那种情形他会认为后来被拉格朗日证明了的事实是理所当然的. 如果这样, 他的直觉并没有欺骗他.

§2.17 结论

这便结束了我们对费马“论数”的著述的分析. 一旦真正地把这些汇拢一起, 它们便呈现出了一幅令人瞩目的协调画面.

他的证明几乎完全消失. 在代数记号仍然极端笨拙, 在规范模式完全缺失的那个时候, 要详细写出那些证明会付出巨大的努力, 而且就其同代人方面来说, 对此完全缺乏兴趣一定也令人非常沮丧.

在他生命的后期, 费马一定害怕他的劳作成果会被丢失. 这里是他给惠更斯最后的信中的伤感结论:

“简明扼要地说, 这些就是我对数的冥思苦想的故事, 我把它记下来只是因为我害怕我会永远找不到空闲来写出和适当推广这些证明和方法. 无论如何, 这将被充作对于从事科学的人们的一个指针, 指引他们自己去找出那些我没有写出来的东西, 特别是如果卡尔卡维与弗莱尼柯大人告诉了他们几个我曾在处理一些负向性命题的课题时使用的下降法证明的话, 更应该去找出它们. 说不定后辈们会因我表明了先辈之人并非知晓一切而感谢我, 用英国的伟大修士 (培根) 的话来说, 这会被我们的后继者们视作‘火炬传递’, 在他的箴言之后我还要补充说: 许多东西都要消逝, 唯科学会成长壮大” [“*Voila sommairement le conte de mes*

resveries sur le suject des nombres. Je ne l'ay escrit, que parce que j'apprehende que le loisir d'estendre et de mettre au long toutes ces demonstrations et ces methodes me manquera. En tout cas cette indication servira aux acavants pour trouver d'eux mesmes ce que je n'estens point, principalement si Monsieur de Carcavi et Frenicle leur font part de quelques demonstrations par la descente que je leur ay envoyees sur le subjet de quelques propositions negatives. Et peut estre la posterité me scaura gré de luy avoir fait connoistre que les anciens n'ont pas tout sceu, et cette relation pourra passer dans l'esprit de ceux qui viendront apres moy pour traditio lampadis ad filios, comme parle le grand Chancelier d'angleterre, suivant le sentiment et la devise du quel j'adjousteray, multi pertransibunt et augebitur scientia"; *Fe*.II,436=*Huy*.II,461–462, August 1659].

无疑更少顺从的、然而或许具有相似气质的伽罗瓦, 在他临死的前夜, 写信给他的朋友 Chevalier 说:" *Après cela il ya aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis*" ("我希望会有一些人出现, 他们将发现所有那些混乱是值得人们去解开的").

然而并没有出现惠更斯以任何方式对费马的信有所回应; 在他 1658 年给沃利斯的信中写道: "我们不缺少能做的更好的东西" (*Huy*.II,211=*Fe*.IV,121), 但立即又补充了对于费马和弗莱尼柯算术工作的更加稳健的评价: "让他们放弃他们的设置问题的做法吧, 学学你的给予我们那些能给他们带来荣誉而给我们带来快乐做法. 依我看来, 确实有一些关于数的奇妙性质非常值得我们去给出证明; 其中之一, 我确信, 就是在 185 页下方费马的信中······" 后者指的是费马给迪格比的最后一封信, 他在那里断言了有关平方数与三角数之和的问题 (*Fe*.II,403–404).

但是, 如果说惠更斯无可争议地比他的同代人更有鉴赏和批评算术工作的能力的话, 他也不准备举起费马递过来的火炬. 只有一次他完全走近了数论; 这出现在他的《*Descriptio Automati Planetarri*》中 (*Huy*.XXI,587–652), 它是在他死后的 1703 年付印但很可能是在 1680 到 1687 年间写成的 (参看索引同上的 p.585). 这里, 在与带齿轮的自动机的实际相关的问题中, 人们发现了建立在连分式算法基础上的, 以分数去最佳逼近实数的完全原创和老练的处理 (索引同上, pp.627–643). 这个沃利斯已触及过的课题最终又被欧拉捡起 (参看, 譬如 *Eu*.I–14,187–215=E71,1737; *Eu*.I-15,31–49=E281,1757, 等等), 后来拉格朗日将此荣誉完全的归到惠更斯的名下, 称其为 "*une des principales découvertes de ce grand géomètre* (这位伟大的几何学家的最重要的发现之一)" (*Lag*.VII,43–44=*Eu*.I–1,536); 但值得注意的是, 惠更斯他自己从来就没有为发表它费过心.

当欧拉在 1730 年捡起费马的火炬并重新点燃它时, 它确实已长时间地熄灭,

而欧拉让它明亮地燃烧了整整下半个世纪. 那个故事将是我们下一章的主题. 这里我们只是注意到, 在花了十余年追寻将关于两个平方数之和的问题弄清却没有取得多少成功之后的 1742 年, 具崇高的声誉的欧拉从柏林写信给巴黎的克莱罗 (Clairaut)*26, 请他去研究所替他查找费马的手稿 (*Eu.*IV,A–5,124; 参看第三章 §4); 按照他所说, "许多秘密可能仍旧隐藏在那里". 回答却令人沮丧 (索引同上, p.129); 按照他给哥德巴赫的报告 (*Corr.*I,168), 由于对于这种事再也没有任何兴趣可言, 查找是没有任何希望的 [" *da der goût für dergleichen Sachen bei den Meisten erloschen ist, so ist auch die Hoffnung verschwunden*"]. 没有任何补救的办法, 除非欧拉自己干. 他这样做了, 并从 1768 年起得到了拉格朗日宝贵的合作. 的确, 到欧拉逝世时, 不仅费马所探索的领地已得以恢复, 而且更广袤的土地也已被征服. 如果一些秘密还存留的话, 它们所涉及的问题必定已超越了费马的认知范围.

费马在一个领域中已经彻底地将他的影像投射到他当前的世纪或者还有下一个世纪. 莱布尼茨已经宣告了它的到来; 这里是他在 1702 年以预言式的洞察写下的:

"……我的希望是那些进一步播撒新科学 (即莱布尼茨的分析学) 种子的人们将会到来, 并且能得到丰硕的收获, 特别地, 如果他们比现在更加勤奋地参与到丢番图代数的推进中就更会如此, 而丢番图代数却因笛卡儿学派没有认识它在几何中的用处被他们所冷落. 另一方面, 我记得我曾反复提到 (某些人似乎对此感到奇怪) 我们的积分学的进展在很大程度上依赖于算术类学科的发展, 就我所知, 是丢番图他首先系统论述了这门学科……" (*Acta Eruditorum* 1702,p.219 = *Math. Schr.* ed. C.I.Gerhardt,(II)Bd.I,Halle 1858,p.360).

以现代术语表示, 莱布尼茨想要说的是, 对代数微分和它们的积分的研究与分类依赖于代数几何的方法, 而在他那个年代只有由丢番图、韦达和费马提供的现存的方法. 他既没有提到韦达也没有提到费马; 或许他根本就没有研习过他们的东西; 然而他的直觉却不会让他迷失方向.

当同一条线索后来首先被欧拉而后被拉格朗日捡起时, 在 "丢番图代数" (莱布尼茨的叫法) 与椭圆积分之间的紧密联系开始以光彩夺目的成功透过表象显现了. 在欧拉反复对他的分析学的同僚们的警示中所明确蕴涵的是, 即便从他们的观点看, 数论不是在浪费光阴. 有时人们可以从他的话里察觉出对前面所引述的莱布尼茨的富于远见评论的反响:

"……作者常常提到的丢番图方法, 如果进一步发展, 则将使整个分析学受益, 所以他对于致力于那个数学分支的持久努力远未感到遗憾……" (*Eu.* E255

*26 1713—1765, 法国物理学家, 主要领域为空间曲线、曲面几何, 以及地球形状的牛顿 - 惠更斯理论等.

中的 I–2,428), 在同一篇文章中他进一步说道: "这表明在丢番图分析中还留有如此多的东西可做, 毫无疑问它对整个分析学, 不管是有限的还是无穷小的, 将有极大的贡献. 事实上, 积分学的一个主要工具在于将无理的微分表达式变换为有理的, 而这可直接由丢番图分析得来, 所以人们完全有理由期待从这个研究中取得深入的进展······" (同上. p.454).

在 1754 年写的那篇文章中, 欧拉在参照了欧几里得对方程 $x^2+y^2=z^2$ 的相应结果后, 用 "丢番图的方法" 证明了三次曲面 $x^3+y^3+z^3=t^3$ 的有理性. 至于对亏格 1 的曲线, 欧拉在其事业初期就已对它们感兴趣 (参看 *Corr.*I,31,1730). 在 1738 年的一篇文章中他范围广泛地论述了它们, 那里他以自己风格重写了费马和弗莱尼柯对于方程 $x^4 \pm y^4 = z^2$ 的论述 (*Eu.*I–2,38–58=E98; 参看前面的 §10), 在那里他还用下降法处理了其他几个同类型的方程, 它们全都属于我们现在称之为 "双纽线" 的情形. 当他早在 1730 年提出了积分 $\int dx/\sqrt{1-x^4}$ 的有理性问题 (*Corr.*I,47,51) 时, 或者在 1751 年年终当他收到法尼亚诺的那篇包含许多关于双纽线的弧长和关于 "双纽线" 积分的不凡的定理的《*Produzioni Matematiche*》(参看第一章 §1) 时, 他立刻认出了这是同一个问题吗? 对此我们没法得知, 但雅各布在 1834 年从圣彼得堡科学院得到欧拉遗作的最后一卷, 它中间包含了许多对形如

$$y^2 = A + Bx + Cx^2 + Dx^3 + Ex^4$$

的丢番图方程的论述. 雅可比由此成功地看出 (*Jac.*II,53) 欧拉的对这些问题的处理等于写出对椭圆积分

$$\int \frac{dx}{\sqrt{A + Bx + Cx^2 + Dx^3 + Ex^4}}$$

的乘法公式, 并且补充说, 这个介于两个理论间的 "令人难忘的一致" ("*consensus ille memorabilis*") 难于逃过 "它们的共同传授人" 的法眼. 对此, 就我们所知, 他没有将其归功于费马, 他对于费马的工作远远没有对欧拉的熟悉; 然而对单独归于与欧拉的事, 他确信是个正确判断. 如果相似情况出现, 他也会对拉格朗日说出同样的话. 拉格朗日在 1766 年从事了对椭圆积分的研究 (*Lag.*II,5–33). 1777 年他写了一篇关于丢番图方程 $2x^4 - y^4 = \pm z^2$ 和与其相关问题的重要文章 (*Lag.*IV,377–398; 参看前面的 §14). 1784 年他又回到了椭圆曲线上 (*Lag.*II,253–312), 写了一篇文章并因其被有时赋予 "重新独立地" 发现了所称作的兰登 (Landen) 变换的名声, 该变换 (或 "同源") 对椭圆积分是二阶的[10]. 难道

[10]譬如参看 A.Enneper 的《*Elliptische Functionen*》(Halle 1876),p. 307. 实际上, 拉格朗日知道兰登 1775 年关于这个主题的文章; 他在 1777 年给 Condorcet的信中引述并简短地评述了它 (*Lag.*XIV,41).

他不会注意到同一个变换是在无限下降法中被费马、欧拉还有在他自己的 1777 年文章中作为主要工具在使用吗 (参看附录 IV)? 的的确确莱布尼茨的语言正在实现.

在十九世纪, 费马的遗产有一次受到了毁灭性的威胁. 从实质上说, 它包含了三个相互关联的原则. 一个是应该研究代数几何, 首先是代数曲线, 不止是在实数域或者最终在复数域上, 同样要在其他的域上, 而且突出地要在有理数域上. 其次一个原则是在这个研究中有理变换是个合适的工具. 第三, 存在可用于丢番图问题的无限下降法. 但是在十九世纪, 代数几何中的函数论式方法的显著成功导致了一时间复数对它竞争者的几乎是全盘的胜利, 这个胜出是从椭圆函数开始的, 它耗尽了对亏格 1 曲线 (这里就是赋予它我们现在所知的这个名称的地点) 的全部研究, 并延续成为黎曼 (Riemann) 的阿贝尔函数理论. 所谓 “纯” 几何的发展, 特别是由彭赛列 (Poncelet) 开创而由沙勒 (Chasles)、默比乌斯 (Möbius) 和其他许多人的发展成的射影几何, 重新恢复了协调和平衡, 如果不是这样, 那么从一开始几乎一成不变的要在复数域上进行操作了; 这个传统在意大利几何中传承下来并有所超越. 在这整个时期中, 费马的名字几乎无一例外地总与他的 “大定理” 即与方程 $x^n + y^n = z^n$ 联系在一起出现, 然而它的丰富成果掌握在库默尔 (Kummer) 的手中, 不属于我们当前的主题.

第一个模糊的反响出现在希尔伯特和赫尔维茨的一篇文章中 (*Acta Math.* 14,vpp.217–224), 在那里第一次明晰地指出, 代数曲线的双有理理论提供了研究丢番图方程的合适架构. 庞加莱 (Poincaré) 在 1901 年对这同一领域作了广泛的纵览, 并且似乎勉强地试图利用椭圆函数的三等分点作为无限下降法的一个工具. 真正的突破是在 1922 年出现的莫德尔 (Mordell) 的著名文章 (*Proc.Cambridge Phil.Soc.* 21,pp.179–192); 在那里, 如果说费马的名字没有出现的话, 那么使用 “无限下降法” 这组字表明莫德尔充分注意到对他遥远年代先辈的亏欠. 自此以后椭圆曲线及其到较高亏格曲线和到阿贝尔簇的推广成了现代数论的一个主要课题. 费马的名字和他的无限下降法牢不可破地与数论绑在了一起; 可以指望它们在未来依旧会如此.

附录 I　欧几里得二次域

如在 §8 与 §12 中指出的那样, 费马关于二次型 $X^2 + AY^2$ (其中 A 为 1 或 ± 2 或 3) 最好用考虑环 $\mathbb{Z}[\theta]$ 来理解, 这里的 θ 是 $i = \sqrt{-1}$, $\sqrt{\pm 2}$, 或 $j = (-1 + \sqrt{-3})/2$. 现在我们来解释它.

在它们的每一种情形中, 我们令 $R = \mathbb{Z}[\theta]$; R 是域 $K = \mathbb{Q}(\sqrt{-A})$ 的整数环. 记 $\xi \mapsto \xi'$ 为 K 的将 $\sqrt{-A}$ 变成 $-\sqrt{-A}$ 的自同构, 并令 $N(\xi) = \xi\xi'$; 称 $N(\xi)$ 为

ξ 的范数. 我们有

$$N(x+y\sqrt{-A}) = x^2 + Ay^2,\ N(x+yj) = x^2 - xy + y^2.$$

在所有的情形我们都有 $N(\xi\eta) = N(\xi)N(\eta)$; 如在第一章 §8 中指出的, 这等价于对于形式 $X^2 + AY^2$ 的基本恒等式, 即第一章 §8 的 (5) 和 (6), 以及第二章 §12 的 (5).

环 R 的单位元是满足 $N(\eta) = \pm 1$ 的 K 中整数 η; 对于 $A = 1$, 它们是 ± 1, $\pm i$; 对于 $A = 2$ 是 ± 1; 对于 $A = 3$ 是 ± 1, $\pm j$, $\pm j^2$. 对于 $A = -2$, 有无限多个单位元, 即所有形如 $\pm\varepsilon^n$ 的元, 其中 $\varepsilon = 1 + \sqrt{2}$, $n \in \mathbb{Z}$ (参看 §12). 称两个整数 α, β 相伴是说每一个在 R 中是另一个倍数; 出现这种情形当且仅当 $\alpha^{-1}\beta$ 是单位元. 称一个非零整数 $\alpha = a + b\theta$ 是正规化的是指, 当 $A = 1$ 时如果有 $a > 0$, $b \geq 0$; 当 $A = 2$ 时如果有 $a > 0$ 或者 $a = 0$, $b > 0$; 当 $A = 3$ 时, 如果有 $a > b \geq 0$; 当 $A = -2$ 时, 如果 $-b < a \leq b$. 在一个给定整数的相伴数中, 有一个且只有一个是正规的; 对于 $A = 1, 2, 3$ 容易看出, 而对于 $A = -2$, 对它的证明本质上就是由费马给出并在前面 §12 中对于方程 $n = 2y^2 - x^2$ 断言 "极小解" (x, y) 存在性的那个证明. 一般说来, 两个正规化整数的乘积并不是正规化的; 可以将此点看作是在 §12 中讨论过的费马的错误的源头.

设 $\zeta = x + y\theta$ 为域 K 中一个任意元; 于是在 K 中至少有一个整数 $\alpha = a + b\theta$ 使得 $|N(\zeta - \alpha)| < 1$; 确实如此, 只要我们取 a, b 分别为最靠近 x 和 y 的有理整数即可. 因此, 如果 α, β 为两个整数, 且 $\beta \neq 0$, 则存在整数 γ, ρ 使得 $\alpha = \beta\gamma + \rho$ 并且 $|N(\rho)| < |N(\beta)|$; 要得到这个, 我们只需要取 γ 使得 $|N((\alpha/\beta) - \gamma)| < 1$ 即可. 然后恰如欧几里得的"书"IV 中的 "欧几里得辗转相除法" 表明在环 R 中存在任意两个整数 α 和 β 的 g.c.d. δ; 像在欧几里得的书中一样, α 和 β 的每个公因子都除尽 δ; 显见, 任何两个这样的正整数必定是相伴的, 从而对于 α, β 有一个且只有一个正规化的 g.c.d. 代替 "欧几里得辗转相除法", 也可以将 δ 取作任意一个数 $\gamma = \alpha\xi + \beta\eta$ 使得 $|N(\gamma)|$ 当 ξ 和 η 取 R 中任意值时具有最小值; 欧几里得辗转相除的过程于是表明了任意一个那样的数是 α 和 β 的 g.c.d.

在环 R 中, 素元定义为那些不等于 0 和单位的整数, 它们除了它们的相伴数和单位外没有其他的因子. 由 g.c.d.的存在性得到, 除尽一个乘积的素元必除尽它的一个因子. 如果 α 是一个整数, 且 $|N(\alpha)| > 1$, 设 π 为它的一个因子使得 $|N(\pi)|$ 取 > 1 的最小值; 这必定是个素数. 由此立刻推出, R 中的每个整数是一些素数和一个单位的乘积而它的这种积表示是 "本质上" 唯一的 (即在差一个单位因子下唯一); 如果规定它的素因子是正规化的, 那么它则是在不计次序下唯一的.

要找出环 R 中的素元我们需要知道 $-A$ 模有理素数的二次剩余特征标; 在

前面的 §7 中 (对 $A=-1$) 和 §12 中 (对 $A=\pm 2$, $A=3$) 它已被确定过. 设 p 是一个有理素数; 如果它在 R 中不是素数, 那么它在 R 中便有素因子 π, 不妨设其为正规化的, 这样, $N(\pi)$ 就是 $N(p)=p^2$ 的一个非 1 非 p^2 的因子, 从而等于 $\pm p$. 现在分别考虑下面四种情形:

(a) 如果 $A=1$, 令 $\pi=x+yi$; 于是 $p=x^2+y^2$, 并且 $p\equiv 1 \pmod 4$ 除非 $p=2$; 在这时有 $\pi=1+i$.

(b) 如果 $A=2$, 令 $\pi=x+y\sqrt{2}$; 于是 $p=x^2+2y^2$, 并且 $p\equiv 1$ 或者 $3 \pmod 8$ 除非 $p=2$; 在这时有 $\pi=\sqrt{-2}$.

(c) 如果 $A=-2$, 令 $\pi=x+\sqrt{2}$, 其中 $-y<x\le y$; 于是 $p=2y^2-x^2$ 并且 $p\equiv 1$ 或者 $7 \pmod 8$ 除非 $p=2$; 在这时有 $\pi=\sqrt{2}$.

(d) 如果 $A=3$, 令 $\pi=x+yj$; 于是 $p=x^2-xy+y^2$. 这里的 x 和 y 不能同为偶数, 故而在 π 的相伴数中, 有一个 (即如果 y 为偶则是 π 自己, 如果 x 为偶则是 πj^2, 如果 x 和 y 均为奇数则是 πj) 必定具有形式 $z+t\sqrt{-3}$, 其中 z 和 t 为整数, 故 $p=z^2+3t^2$; 我们有 $p\equiv 1 \pmod 3$ 除非 $p=3$. 在这时 p 具有素因子 $\sqrt{-3}$ (或者以正规化形式的 $2+j=-j\sqrt{-3}$).

如果如上, p 不是素元, 而 π 是 p 的一个素因子, 又设 π' 也是个素因子; 容易验证, 除了 $p=2$ (在情形 (a),(b),(c)) 或者 $p=3$ (在情形 (d)) 外, π' 不可能是 π 的一个相伴数. 置后一种情形不顾, 则在每种情形中 p 都是一个 "形如 X^2+AY^2 的因子" (在前面的 §12 有定义), 或者意思是一样的, $-A$ 是模 p 二次剩余. 至于其逆, 假定 p (如果 $A=1$ 或 ± 2 则不是 2, 如果 $A=3$ 则不是 3) 是形如 X^2+AY^2 的因子; 这表明 p 除尽某个整数 a^2+Ab^2, 其中 a 和 b 与 p 互素; 因为没有一个整数 $a\pm b\sqrt{-A}$ 在 R 中是 p 的倍数, 这表示 p 在 R 中不是一个素数.

将一个整数表示为形式 X^2+AY^2 的个数问题现在可以明确阐述为当将 R 中相伴数看作相同时, 这是 R 中范数为 N 的元素个数; 用现代词语表示它等于是决定域 $K=\mathbb{Q}(\sqrt{-A})$ 的 ζ 函数. 由于所考虑的各种情形十分相似, 那么只要考察 $A=1$, $R=\mathbb{Z}[i]$ 的情形就够了. 我们必须解 $N=\alpha\alpha'$. 如果 N 有一个形如 $4n-1$ 的素因子 p, 则由于 p 在 R 中仍为素数, 它必定除尽 α 或 α' 从而必定同时除尽这两个, 故 N 是 p^2 的一个倍数; 这给出了 $p^{-2}N=(\alpha/p)(\alpha'/p)$. 这样便把问题化到 N 没有这类素因子的情形. 于是我们可将其写成

$$N=2^s p_1^{r_1}\cdots p_m^{r_m},$$

其中每个 p_i 具有形式 $4n+1$, 从而可写成 $\pi_i\pi_i'$, 这里 π_i 在 R 中为素数. 对于任意的 i, 设 λ_i, μ_i 分别为 π_i, π_i' 在 α 中的指数; 它们也是 π_i', π_i 在 α' 中的指数,

记 $\lambda_i + \mu_i = r_i$, 于是 α 必定由

$$\alpha = (1+i)^s \pi_1^{\lambda_1} \pi_1'^{\mu_1} \cdots \pi_m^{\lambda_m} \pi_m'^{\mu_m}$$

给出. 对 α 的可能的选取个数可清楚看出为 $\prod(r_i+1)$. 对于 N 为形如 X^2+Y^2 的表示个数必定是前面这个数的一半, 这是因为 α 和 α' 给出了同一个表示. 这个表示在 §9 中的意义下为 " 正常" 的当且仅当对所有的 $\lambda_i = 0$ 或者 $\mu_i = 0$, 这是因为否则 α 就会是 p 的一个倍数; 因此正常表示的个数为 2^{m-1}. 所有这些当然与在 §9 中所叙述的费马的研究一致.

我们现在可以利用环 $\mathbb{Z}[\sqrt{2}]$ 来解释和厘清费马在 1657 年给弗莱尼柯信中的疑问了 (*JEH.* 41–44; 参看前面的 §12). 设 $\pi = a + b\sqrt{2}$ 为一个正规化的整数满足 $0 < a < b$; 令 $\rho = \varepsilon\pi'^2 = A + B\sqrt{2}$; 这给出了

$$A = a^2 + 2b^2 - 4ab,\ B = a^2 + 2b^2 - 2ab,$$

容易看出 ρ 是正规化的. 现假定 p 为形如 $p = 2x^2 - 1$ 的有理素数, $p^2 = 2y^2 - 1$. 令 $a = 1$, $b = x$, 故 $p = -\pi\pi'$; 于是 π, π' 为 R 中的素数. 令 $\omega = 1 + y\sqrt{2}$, 故 $\omega\omega' = -p^2 = -\pi^2\pi'^2$; 由于 π, π' 为素数, 并因为 ω 不是 p 的倍数, 这表明 ω 是 π^2 或 π'^2 的, 或者等于说, 是 ρ 或 $-\rho'$ 的一个相伴数. 但 ω, ρ, $-\rho'$ 是正规化的; 因此 ω 必是 ρ 或 $-\rho'$, 从而恰如在 §12 那样, 得到 $1 = \pm(1 + 2x^2 - 4x)$, 于是 $x = 1$ 或 2. 如果 p 不是素数, 这个证明显然是不能使用的, 尽管费马做过相反的断言 (参看 §12).

附录 II 射影空间中的亏格 1 曲线

我们已经看到, 大多数费马所研究过的丢番图问题涉及的方程或方程组, 我们现在会说, 它们定义了椭圆曲线, 即亏格为 1 的代数曲线; 在每个情形中的问题都是求该曲线上的有理点 (有时是整点). 为了真正了解他的方法, 将它们转换成现在在代数几何中通常使用的语言将是方便的.

在这里我们必须说的许多话, 实际是许多费马关于这个课题的工作, (参看前面的 §15) 都是在任意的基域上仍然保持有效的, 甚至包括那些特征 $p > 1$ 的域; 为了使言语简明, 我们将忽略后面的这种情形. 就费马所关心的范围而言, 与实数域 $\mathbb{R}$ (在他的年代理解为 "几何" 的域)、有理数域 $\mathbb{Q}$ 以及隐含着的所有代数数域都有关联.

设 Γ 为一条代数曲线; 我们假定它不可约并由系数在复数域 $\mathbb{C}$ 的一个子域 K 中的一些方程定义. 我们将 Γ 的一个点理解为坐标在 $\mathbb{C}$ 中的点; 如果它的坐标在 K 中则称其为有理点, 如果它们是在 K 上代数的则称该点为代数的. 一

个除子是指一个形式和 $\mathfrak{a} = \sum a_i A_i$, 其中 A_i 是 Γ 的点, 而 a_i 为整数; 称 $\sum a_i$ 为 $\mathfrak{a}$ 的次. 如果所有的 $a_i \geq 0$, 则称 $\mathfrak{a}$ 为正的, 记为 $\mathfrak{a} \succ 0$. 如果 P_1 是 Γ 的一个代数点, 而 $P_1, P_2, \cdots, P_n$ 是它在 K 上的全部不同的共轭点, 称除子 $\sum P_i$ 是素有理的 (在 K 上); 称一个除子为有理的是指, 如果它是素有理除子的整系数线性组合. Γ 上的有理函数 $f(M)$ 则理解为 Γ 上点 M 坐标的一个有理函数; 称它为在 K 上有理的, 是说如果它的系数是在 K 中. 我们按通常的方式定义 Γ 上函数的极点和零点; 每个函数具有同样多个极点和零点, 其中每个点的点数是按其重数计算的. 如果 f 的零点为 $A_1, A_2, \cdots, A_n$, 极点为 $B_1, B_2, \cdots, B_n$, 则称 $\sum A_i - \sum B_i$ 为 f 的除子, 记为 $\operatorname{div}(f)$; 它的次数为 0; 如果 f 在 K 上为有理的, 则 $\operatorname{div}(f)$ 也是有理的; 如果除子 $\mathfrak{a}$ 是某个函数 f 的除子, 则称其等价于 0, 记为 $\mathfrak{a} \sim 0$. 于是两个除子间的等价性可按通常方式写出.

称曲线 Γ 是亏格 1 的 (或 "椭圆的") 是说如果对 Γ 上每个次数为 1 的除子 $\mathfrak{a}$, 有且只有一个点 A 使得 $A \sim \mathfrak{a}$; 自此之后我们总假定有此条件. 于是, 如果 $\mathfrak{m}$ 是 Γ 上的一个 $m > 0$ 次的有理除子, Γ 上那些 K 上的函数 f, 它们在 K 上有理并使得 $\operatorname{div}(f) \succ -\mathfrak{m}$ (特别是如果 $\mathfrak{m} = \sum M_i$ 时以 $M_1, M_2, \cdots, M_m$ 为极点的函数) 构成一个 K 上的 m 维向量空间. 特别地, 如果 $m = 1$, 函数 f 在差一个常数因子下唯一, 而它的除子是 $\operatorname{div}(f) = N - \mathfrak{m}$, 其中 N 是使得 $N \sim \mathfrak{m}$ 的点; 这个点 N 因此是由函数的零点得到的, 于是必定为有理的.

因此, 如果在 Γ 上有一个次数 1 的有理除子则必定在 Γ 上至少有一个有理点 A. 这时 Γ 上有理于 K 的函数 f 使得 $\operatorname{div}(f) \succ -2A$ (分别地, $\succ -3A$) 构成一个 K 上的二维 (分别地, 三维) 向量空间 V (分别地, W). 任取一个非常值的 $x \in V$; 于是 V 由函数 $\alpha x + \beta$ 组成, 其中 α, β 属于 K; 相似地, 如果我们取 y 在 $W - V$ 中, W 则由函数 $\lambda y + \mu x + \nu$ 构成, 其中 λ, μ, ν 属于 K. 适当选取 V 中的 x 和 W 中的 y, 我们可假定它们满足一个形如

$$y^2 = x^3 - ax - b$$

的方程, 其中 a, b 在 K 中; 这里的右端没有重根, 因为否则的话它不再定义一条椭圆曲线了. 于是可以将 Γ 等同于由该方程定义的平面三次曲线, 或者更恰当地说成是等同于射影平面 P^2 上由齐次方程

$$Y^2 Z = X^3 - aXZ^2 - bZ^3$$

定义的三次曲线, 而 A 于是成了在该三次曲线上的无穷远点 $(0,1,0)$. 如果 M, N, P 为该三次曲线上的三个点, 那么它们处在同一条直线上当且仅当 $M + N + P \sim 3A$; 特别地, 如果对于该曲线上每个 $P = (x, y)$, 我们记 $P' = (x, -y)$, 则有 $P + P' \sim 2A$. 如果对该曲线上每对点 (M, N), 我们定义一个点 $M \dotplus N$ 为

$M \dotplus N \sim M + N - A$, 规则 $(M, N) \mapsto M \dotplus N$ 将 Γ 上点的集合定义成了一个交换群, 其中的有理点构成了一个子群, A 作为了单位元; 在处理一条给定的三次曲线时, 可以以 $M + N$ 代替 $M \dotplus N$, 以 0 代替 A. 我们有 $P = M \dotplus N$ 当且仅当 M, N, P' 在同一直线上, 即如果 P' 是通过 M, N 的直线与此三次曲线相交的第三个点. 相似地, $M \dotplus M$ 是点 P 使得 P' 为该曲线在 M 的切线与该曲线的交点, 同样地, 记 $M \dotplus M$ 为 $2M$.

现在只假定 Γ 有一个二次有理除子 $\mathfrak{a} = A + A'$; 我们又一次在 Γ 上取一个非常值的 x, 它在 K 上有理, 使得 $\mathfrak{a} + \mathrm{div}(x) \succ 0$. 有理于 K 的函数使得 $2\mathfrak{a} + \mathrm{div}(f) \succ 0$ 的全体是一个四维空间 W, 它包含了一个由 1, x, x^2 生成的子空间 W'; 取 y 属于 W 但不属于 W'. 用 $y + \lambda x^2 + \mu x + \nu$ 代替 y, 其中 λ, μ, ν 取适当的值, 这之后, 我们有方程

$$y^2 = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4,$$

这里右端没有重根; 这可看成是曲线 Γ 的定义方程. 在一种显然的意义下, 构成除子 $\mathfrak{a}$ 的两个点 A, A' 是该曲线上的无穷远点; 它们是有理的当且仅当 a_0 在 K 中是个平方元.

类似地, 如果 Γ 有一个次数 $m \geq 3$ 的有理除子 $\mathfrak{a}$, 取所有在 K 上有理的、使得 $\mathfrak{a} + \mathrm{div}(f) \succ 0$ 的函数 f 构成的空间中的一组基 $(x_1, \cdots, x_m)$; 以下面的方式将 Γ 映到 $m-1$ 维射影空间 P^{m-1} 中: 对 Γ 的每个点 M, 取 P^{m-1} 中具齐次坐标

$$(x_1(M), \cdots, x_m(M))$$

为在此映射下的像点. 于是 Γ 在 P^{m-1} 中的像是 P^{m-1} 中的一条 m 次曲线 Ω. 它与超平面

$$a_1X_1 + \cdots + a_mX_m = 0$$

的交由 $P_1, \cdots, P_m$ 组成, 它们由

$$\mathrm{div}\left(\sum_1^m a_ix_i\right) = \sum_i^m P_i - \mathfrak{a}$$

给出, 而且 Γ 上 m 个点落在一个超平面上当且仅当 $\sum_1^m P_i \sim \mathfrak{a}$. 如果 $m = 3$, 我们因此得到 Γ 的一个平面三次曲线的模型; 如果 $m = 4$ 则得到了一个空间的四次曲线的模型 Ω. 在后面这个情形中, 考虑 10 个函数 x_ix_j, $1 \leq i \leq j \leq 4$; 它们是在满足 $2\mathfrak{a} + \mathrm{div}(f) \succ 0$ 的函数 f 构成的空间中的; 由于这个空间的维数为 8, 于是在 x_ix_j 之间存在两个线性关系; 这等于是说 Ω 是两个二次超曲面 $\Phi(X) = 0$ 与 $\Psi(X) = 0$ 的交, 这里的 Φ, Ψ 是两个对 X_i, X_j 的二次型.

最后假定我们在 Γ 上有两个不等价的二次有理除子 $\mathfrak{a} = A+A'$, $\mathfrak{b} = B+B'$; 取两个在 K 上有理的非常值函数 x, y 使得 $\mathfrak{a} + \mathrm{div}(x) \succ 0$, $\mathfrak{b} + \mathrm{div}(y) \succ 0$. 考虑 9 个函数 $x^i y^j$, $i,j \leq 2$; 它们都在由满足 $2\mathfrak{a} + 2\mathfrak{b} + \mathrm{div}(f) \succ 0$ 的函数 f 构成的空间中; 由于此空间的维数等于 8, 故在这些 $x^i y^j$, $i,j \leq 2$ 必有一个线性关系 $F(x,y) = 0$, 其中 F 是个对 x 和 y 的次数 ≤ 2 的多项式. 这里的 y 必定出现在 F 中否则 x 就会是常值; 同样 x 也必出现其中. 如果 F 对 y 的次数为 1, y 就会具有 $R(x)$ 的形式, 其中的 R 为一个有理函数. 但是容易看出, y 的极点除子就会线性等价于 $\mathfrak{a}$ 的一个倍除子 $m\mathfrak{a}$. 如果 $m > 1$, 这与 $\mathfrak{b} + \mathrm{div}(y) \succ 0$ 的假定矛盾; 如果 $m = 1$, 则同样会导出矛盾, 这是因为 $\mathfrak{b}$ 不等价于 $\mathfrak{a}$. 因此我们有关系式

$$F(x,y) = 0,$$

其中 F 对 x 和对 y 的次数都是 2. 欧拉是第一个考虑这种类型丢番图方程的人 (下文的附录 V, 以及第三章 §14).

附录 III 作为空间四次曲线的费马的“二重方程”

在我们对费马和欧拉研究过的“二重方程”以及他们所使用的无限下降法进行讨论时, 我们将需要关于亏格为 1 的空间四次曲线的一些初等事实. 设 Ω 为这样的一条曲线; 我们在附录 II 中已经看到, 它可以被一对方程 $\Phi = \Psi = 0$ 定义, 其中 $\Phi = 0$ 和 $\Psi = 0$ 是 P^3 中两个二次曲面的方程. 对任意 ξ 记由 $\Phi - \xi\Psi = 0$ 给出的二次曲面为 Q_ξ; 这些二次曲面构成通过 Ω 的二次曲面束 (当然也包含了二次曲面 $\Psi = 0$, 可记其为 Q_∞).

对于任意一个二次型

$$\Phi = \sum_{i,j=1}^{4} a_{ij} X_i X_j,$$

我们记 $\det(\Phi) = \det(a_{ij})$. 一个行列式为 δ 的齐次坐标变换将 $\det(\Phi)$ 乘上了 δ^2; 如果将 Φ 乘以常数 λ, 则 $\det(\Phi)$ 便被乘以 λ^4; 因此当二次曲面 $\Phi = 0$ 给出时, $\det(\Phi)$ 被确定到一个平方因子. 对于上面这样的 Φ, Ψ 我们记 $F(\xi) = \det(\phi - \xi\Psi)$. 对于 $F(\xi) = 0$, Q_ξ 是一个锥面; 如果 Ω 是空间四次曲线, 这个锥不会退化为一对平面. 无疑“束” $\{Q_\xi\}$ 必定至少包含一个锥面, 不妨假定其为 Q_0; 于是 0 是 F 的一个根; 取坐标使得 $\Phi = X_3^2 - 2X_1X_2$, 容易看出 0 不会是 F 的一个重根除非二次曲面 $\Psi = 0$ 通过了锥 Φ 的顶点 $(0,0,0,1)$, 在这种情形 Ω 的亏格为 0 而不是 1. 因此 F 的次数或为 4 或为 3, 并有 4 个在同一条射影直线上的不同零点; 换句话说, 通过 Ω 的二次曲面束恰好包含了四个锥面.

现在我们来概述下面结果的一个证明:

命题. 存在一个从 $\Omega \times \Omega$ 到曲线 $F(\xi) = \eta^2$ 的一个有理映射 ω 使得: (i) 如果 M, M', N, N' 是 Ω 上的 4 个点, 则 $\omega(M, M') = \omega(N, N')$ 当且仅当 $M + M' \sim N + N'$; (ii) 如果 A 是 Ω 上的一个有理点, 则映射 $M \mapsto \omega(A, M)$ 是 Ω 到曲线 $F(\xi) = \eta^2$ 上的一个同构.

为方便起见, 我们从回顾一些众所周知的事实着手:

引理. 一个 (不是一对平面) 二次曲面 $\Phi = 0$ 按照 $\det(\Phi)$ 为 0 与否决定具有一个直线族还是两个; 如果含有一条有理直线, 则 $\det(\Phi)$ 是个平方数.

如果 $\det(\Phi) = 0$, 这个二次曲面是个锥面从而上述断言显然成立. 如果 $\det(\Phi) \neq 0$, 则在适当地扩张基域后可假定该二次曲面包含了一个有理点 A; 取坐标使得 $A = (0,0,0,1)$ 并使在 A 的切平面为 $X_3 = 0$; 如有必要在另一个有理坐标变换下, 在差一个常数因子的条件下写成

$$\Phi = X_1^2 - dX_2^2 - 2X_3X_4;$$

其中 $\det(\Phi) = d \neq 0$. 于是 A 位于两条直线 $X_1 = \pm X_2\sqrt{d}$, $X_3 = 0$ 之上. 特别地, 如果我们假定了该二次曲面包含了一条有理直线的话, 那么我们便能选取 A 为在此直线上的一个有理点, 并依上述而行, 则 $\sqrt{d}$ 便必定为有理的, 从而 $\det(\Phi)$ 便必定是一个平方数. 无论哪种情形, 这两条通过 A 的直线分别属于下面两个族:

$$t(X_1 \pm X_2\sqrt{d}) = uX_3, \quad u(X_1 \mp X_2\sqrt{d}) = 2tX_4.$$

无疑该二次曲面的每个点都位于这两个直线族中每个族的一条且只有一条直线上; 这意味着在此二次曲面上的所有直线属于这两个族中的这个或另一个.

现在回到由 $\Phi = \Psi = 0$ 定义的四次曲线 Ω 上, 在 Ω 上取两个点 M, M'; 记通过两点 M, M' 的直线为 $\Delta_{MM'}$ (或者 Ω 在 M 的切线, 这时 $M = M'$). 如果二次曲面 $\Phi - \xi\Psi = 0$ 包含了 $\Delta_{MM'}$ 上除 M, M' 以外的点, 则它必包含了 $\Delta_{MM'}$; 因此 Φ/Ψ 在 $\Delta_{MM'}$ 为常值, 记此值为 $\xi(M, M')$; 显见这是一个 M 和 M' 坐标的有理函数, 其系数在基域 K 中. 由于此引理, 在将 M 和 M' 的坐标添加到基域后, $F[\xi(M, M')]$ 必定是个平方数; 因此存在那些坐标的有理函数 $\eta(M, M')$ 使得

$$F[(\xi(M, M')] = \eta(M, M')^2.$$

记 Γ 为曲线 $F(\xi) = \eta^2$, ω 为从 $\Omega \times \Omega$ 到 Γ 的映射

$$(M, M') \mapsto (\xi(M, M'), \eta(M, M'));$$

我们要证明它具有上面所叙述的性质. 从 (ii) 开始.

像在附录 II 中那样, 取基域 K 使得 Φ 和 Ψ 的系数均在其中; 假定在 Ω 上有一个坐标在 K 中的点 A. 对于任意 ξ, 取 η 使得 $\eta^2 = F(\xi)$. 设 Δ 为通过 A

并在 Q_ξ 上的直线中的一条; 像在引理的证明中所显示的那样, 它在 $K(\xi,\eta)$ 上为有理. 对于不同于 A 的一个点 P 也具此性质, 这个点 P 是 Δ 与不同于 Q_ξ 的族 $\{Q_\xi\}$ 中的一个二次曲面的交点, 不妨就设此二次曲面为 $\Phi=0$. 因为 P 在 Ω 上, 我们便有 $\Delta=\Delta_{AP}$, $\xi(A,P)=\xi$, 从而 $\eta(A,P)=\pm\eta$; 如有必要将 η 换作 $-\eta$, 因此可设 $\eta(A,P)=\eta$, 故 $\omega(A,P)=(\xi,\eta)$. 因为同时 P 还是在 $K(\xi,\eta)$ 上为有理的, 这证明了 $P\mapsto\omega(A,P)$ 确实是一个从 Ω 到 Γ 的双有理映射, 从而是个同构. 特别地, 这证明了 $\omega(A,P)=\omega(A,P')$ 蕴含了 $P=P'$, 这个结论即便当 A 不是有理时仍然成立, 这是因为我们总可以扩大 K 使得它为有理.

现在在 Ω 上取 M, M', P; 令 $\omega(M,M')=(\xi,\eta)$. 记 P' 为 Ω 与通过 M, M', P 的平面 Π 相交的第四个点; 令 $\mathfrak{a}=M+M'+P+P'$. 由于 $\Delta_{MM'}$ 和 $\Delta_{PP'}$ 都在 Π 上, 它们交于一个点 R. 二次曲面 Q_ξ 包含了 $\Delta_{MM'}$, 从而包含了 R, 从而包含了 $\Delta_{PP'}$; 因此我们有 $\xi(P,P')=\xi$.

设 N, N' 也为 Ω 上的两个点; 我们有 $N+N'\sim M+M'$ 当且仅当 $N+N'+M+M'\sim\mathfrak{a}$; 在附录 II 中已经证明, 这个关系成立当且仅当 N, N', P, P' 共面; 如果这样, 上面的证明表明我们有 $\xi(N,N')=\xi(P,P')=\xi$, 从而 $\eta(N,N')=\pm\eta$. 现让 M, M' 保持不动, 而取 N 为变量; 由于 $\eta(N,N')$ 是用 N,N' 有理地给出, 并且因为 η 是常值, 故 $\eta(N,N')$ 必与 N 无关. 取 $N=M$, 我们得到 $N'=M'$. 因此 $\eta(N,N')=\eta$, 从而如所断言, $\omega(N,N')=\omega(M,M')$.

反之, 假设 $\omega(N,N')=\omega(M,M')$, 并取 N'' 使得 $N+N''\sim M+M'$. 于是有

$$\omega(N,N'')=\omega(M,M')=\omega(N,N').$$

如上所证, 这表明 $N''=N'$, 从而完成了我们的命题证明. 我们的结果可以解释为 Ω 上的次数为 2 的除子等价类被 Γ 参数化.

我们的命题譬如可以应用到以丢番图和费马的语言所说的“二重方程”

$$ax^2+2bxy+cy^2=z^2,\quad a'x^2+2b'xy+c'y^2=t^2$$

定义的曲线上. 由于他们只考虑了那种在射影空间中至少有一个“可见”有理点的曲线, 出于当前目的, 这也是我们的假定. 于是我们看到了该曲线同构于由

$$Y^2=X[(b'X-b)^2-(a'X-a)(c'X-c)]$$

定义的一条曲线. 试举问题

$$x^2+4y^2=z^2,\quad x^2+y^2=t^2$$

为例; 对此欧拉证明了 (参看前面的 §16) 存在显然解以外的解. 我们看出这些

方程定义了一条同构于

$$Y^2 = -X(X-1)(X-4)$$

的曲线. 另一方面举由费马考虑过的一个问题 (参看 §16) 即组成算术级数的四个平方数为例. 这等价于

$$2y^2 = x^2 + z^2, \quad 2z^2 = y^2 + t^2.$$

由上面相同的规则知, 这条曲线同构于

$$Y^2 = X(X+2)(2X+1),$$

将 X, Y 替换为 $-\frac{1}{2}X, \frac{1}{2}Y$, 就把它化成了早先的方程. 因此如欧拉所揭示的那样: 这两个问题是等价的.

附录 IV 下降法与莫德尔定理

我们现在的目的是要为费马的 "下降法" 提供一个基于这个课题的现代工作背景[11], 这是个他在处理椭圆曲线时使用的方法 (参看前面 §16).

在附录 II 中已经知道, 如果一条椭圆曲线至少有一个有理点, 那么它就可以被表现为三次曲线 $y^2 = f(x)$, 其中 f 是个三次多项式. 这条三次曲线上的有理点构成一个群, 而费马的下降法被莫德尔在 1922 年进行了提炼, 使得可用它来证明这个群是 "有限生成的", 这意味着在此三次曲线上有有限个有理点使得其他的有理点可由它们通过在附录 II 中定义的运算生成. 如果不用有理数域 $\mathbb{Q}$ 而用 $\mathbb{Q}$ 上的有限次的任意代数数域作为基域, 这个结果仍然成立. 设 r 为使得在该三次曲线上不满足任何非零整系数线性关系的有理点个数中的最大整数; 我们称 r 为该曲线的秩. 甚至现在也不知道有什么系统的方法来决定一条已知三次曲线的秩, 更不要提这个有理点群的生成元组了.

为简明起见我们考虑 f 的根为有理整数 α, β, γ 的情形, 此时, 三次曲线 Γ 由

$$(1) \qquad y^2 = f(x) = (x-\alpha)(x-\beta)(x-\gamma)$$

给出. 令 $x = X/Z$, 其中 Z 是个自然数, X 为与 Z 互素的整数. 这给出了

$$(Z^2y)^2 = Z(X-\alpha Z)(X-\beta Z)(X-\gamma Z).$$

[11] 譬如参看 J.W.S.Cassels, *J.London Math.Soc.*41(1966),pp.193–291, 以及 A.Weil, *Coll.Papers* I.47–57.

因为 Z 与右端的其他因子互素它必定为平方数, 记 $Z=T^2$. 按惯例我们注意到这些因子中任两个的 g.c.d. 均除尽一个固定的整数, 从而可以将其写成 $X-\alpha Z=AU^2$, 其中只容许 A 取有限多个值, 因此 $x-\alpha=Au^2$, 其中 $u=U/T$, 相似地, $x-\beta=Bv^2$, $x-\gamma=Cw^2$, 其中的 u,v,w 为有理数, 而 B,C 只能取有限多个值. 如果我们只运用这些关系中的第一个便可得到四次曲线

$$z^2=A(Au^2+\alpha-\beta)(Au^2+\alpha-\gamma)$$

的一个有理点 $(u,z=y/u)$, 它因此是属于 Γ 的有限个点中的一个. 另一方面, 适当地选取 u, v, w 的符号后, 我们可以写出

$$(2)\qquad Au^2+\alpha=Bv^2+\beta=Cw^2+\gamma,$$

$$(3)\qquad x=Au^2+\alpha,\quad y=\sqrt{ABC}\cdot uvw.$$

这里的 ABC 必为平方数; (2) 定义了一条在 (u,v,w)- 空间中的四次曲线 Ω, 而 (3) 定义了一个从 Ω 到 Γ 的映射. 原来的问题因而化成了在有限条这类四次曲线上找有理点的问题了. 这些方法中任何一个都是典型的传统下降法.

现在我们将等价于上述方法但却更与现代理论相协调的另一种方法叙述如下. 设 (x,y) 为方程 (1) 的一个解; 我们可以以一种也仅有的一种方式记 $x-\alpha=Au^2$, $x-\beta=Bv^2$, $x-\gamma=Cw^2$, 其中 u, v, w 为有理数, 并且 A, B, C (可正可负) 不含平方因子; 要使方程 (2)(3) 得到满足, 则 ABC 必为平方数.

对于使得 ABC 为平方数的不含平方因子的任意整数 A, B, C (可正可负), 记 $\Omega(A,B,C)$ 为由 (2) 定义的空间四次曲线. 在下降法中的第一步在于将 (1) 由此化为在无限多条四次曲线 $\Omega(A,B,C)$ 上找有理点. 下一步则是丢弃除有限条外所有的这些四次曲线, 因为它们不可能有有理点.

在齐次坐标下, $\Omega(A,B,C)$ 可看为由方程

$$(4)\qquad AU^2+\alpha T^2=BV^2+\beta T^2=CW^2+\gamma T^2$$

定义; $\Omega(A,B,C)$ 具有有理点当且仅当 (4) 具有一个没有公因子的整数解 U, V, W, T; 对此的一个必要条件显然是对于任给的 m, 原来的关系看成是模 m 的同余式时应该有这样的解. 使用 p 进域的术语, 这可表达为 (2) 应该在每个 p 进域 $\mathbb{Q}_p$ 中有一个非平凡解; 我们还可对此加上条件: 应该在实数域 $\mathbb{R}=\mathbb{Q}_p$ 中有非平凡解.

特别地, 取 B 和 C 的一个公共素因子 p; 由于 ABC 是一个平方数且 A, B, C 不含平方因子, 故 p 不除尽 A. 取 $m=p^2$, 并设 p 不除尽 $\beta-\gamma$;

那么同余式

$$AU^2+\alpha T^2 \equiv BV^2+\beta T^2 \equiv CW^2+\gamma T^2 \pmod{p^2}$$

首先表明 p 除尽 T, 然后则表明它除尽 U, 再后则除尽 V 和 W; 于是 $\Omega(A,B,C)$ 不可能有有理点 (即便在 $\mathbb{Q}_p$ 上也没有). 因此, 如果 $\Omega(A,B,C)$ 上有有理点, 并且如果记 B 和 C 的 g.c.d. 为 a, 则 a 必除尽 $\beta-\gamma$. 现在记 $B=ab$, $C=ac$, 其中 b 与 c 互素; 则我们一定有 $A=bc$. 由于 B 和 C 不含平方因子, a 与 b 和 c 互素, 故 $|b|$ 是 A 和 C 的 g.c.d., 而 $|c|$ 是 A 和 B 的 g.c.d.; 因此 b 除尽 $\gamma-\alpha$, c 除尽 $\alpha-\beta$.

这样便留下了有限多条曲线 $\Omega(A,B,C)$, 再进一步在实数域上进行论证和考虑, 这会再去掉一些; 甚至可能除那些具有点在所有 $\mathbb{Q}_p$ 和 $\mathbb{R}$ 的曲线外全都被丢弃. 但是, 与返回到勒让德 (参看第四章 §6) 时的关于亏格 0 曲线的经典结果相对比, 既不是所有的这种四次曲线都有有理点, 也不是当这种点存在时就有已知的方法来找到它. 为了进一步进行下去, 现在假定在全部四次曲线 $\Omega(A,B,C)$ 中除四次曲线 $\Omega(A_i,B_i,C_i)$ $(1\le i\le n)$ 含有至少一个有理点外, 其他的都不含有. 于是, 如果 $M=(x,y)$ 是 Γ 上任意一个有理点, 则存在且只存在一个 i 使得对于 $A=A_i$, $B=B_i$, $C=C_i$ 以及对 u, v, w 的某些有理数值关系式 (2) 和 (3) 被满足; 在这种情况下, 我们说 M 属于 Ω_i, 并说它对应于 Ω_i 上的点 $N=(u,v,w)$.

设 $\Omega=\Omega(A,B,C)$ 为一个 Ω_i; 不去使用 (2) 定义它, 而是记

$$\begin{aligned}\Phi(U,V,W,T) &= \alpha(\beta-\gamma)(AU^2+\alpha T^2)+\beta(\gamma-\alpha)(BV^2+\beta T^2)\\ &\quad+\gamma(\alpha-\beta)(CW^2+\gamma T^2)\\ &= \alpha(\beta-\gamma)AU^2+\beta(\gamma-\alpha)BV^2\\ &\quad+\gamma(\alpha-\beta)CW^2-\delta T^2,\\ \Psi(U,V,W,T) &= (\beta-\gamma)AU^2+(\gamma-\alpha)BV^2+(\alpha-\beta)CW^2,\end{aligned}$$

其中我们已令

$$\delta=(\beta-\gamma)(\gamma-\alpha)(\alpha-\beta);$$

于是 Ω 可看为是由 $\Phi=\Psi=0$ 定义的. 依照附录 III 的记号, 我们有

$$\begin{aligned}F(\xi)=\det(\Phi-\xi\Psi) &= \delta^2 ABC(\xi-\alpha)(\xi-\beta)(\xi-\gamma)\\ &= \delta ABC\cdot f(\xi).\end{aligned}$$

对 Ω 上任意一对点 N, N', 设 $\xi(N,N')$, $\eta(N,N')$ 如附录 III 中所定义的那样; 令

$$\omega_0(N,N')=(\xi(N,N'),\ (\delta\sqrt{ABC})^{-1}\eta(N,N')),$$

故 ω_0 将 $\Omega\times\Omega$ 映到 Γ.

设 $M=(x,y)$ 为 Γ 上属于 Ω 的一个点, 并且对应于 Ω 的一个点 $N(u,v,w)$, 使得关系式 (2) 和 (3) 被满足, 而 Ω 在 N 的切线 Δ_{NN}, 它通过了由 $Auu'=Bvv'=Cww'$ 给出的具齐次坐标 $(u',v',w',0)$ 的点. 因此 $\xi(N,N)$ 由

$$\xi(N,N)=\frac{\Phi(u',v',w',0)}{\Psi(u',v',w',0)}$$

给出. 简单的计算给出 $\xi(N,N)=x$; 于是我们有

$$\eta(N,N)^2=F(x)=\delta^2ABCf(x)=\delta^2ABCy^2.$$

因为根据在附录 III 中的定义, η 只定义到差一个因子 ±1, 如有必要我们便可以假定 $\eta(N,N)=\delta\sqrt{ABC}\cdot y$, 使得 $\omega_0(N,N)=M$. 如果记 λ 为映射 $N\mapsto\omega_0(N,N)$, 这表明 λ 就是由 (3) 定义的从 Ω 到 Γ 的映射.

现在在 Γ 上选取一个有理点 M_0, 它属于 Ω 并对应于 Ω 上一个点 N_0; 按定义, 这表示 $\lambda(N_0)=M_0$. 记 μ 为从 Ω 到 Γ 的映射 $N\mapsto\omega_0(N_0,N)$; 附录 III 中的命题表明这是一个从 Ω 到 Γ 上的同构; 以 μ^{-1} 记其逆, 我们有 $\mu(N_0)=\lambda(N_0)=M_0$. 在 Γ 上任取一点 M; 令 $P=\mu^{-1}(M)$, 故 $M=\mu(P)$. 按定义, M 属于 Ω 并对应于 Ω 上的一个点 N 当且仅当 (3) 将 N 映成 M, 即当且仅当 $\lambda(N)=M=\mu(P)$, 即, 如果考虑到 λ 和 μ 的定义, 当且仅当 $\omega_0(N,N)=\omega_0(N_0,P)$. 再一次运用附录 III 的命题, 我们知道, 上述成立当且仅当在 Ω 上有 $2N\sim N_0+P$. 令 $M'=\mu(N)$; 由于 μ 是一个同构并将 N, N_0, P 分别映成 M', M_0, M, 关系式 $2N\sim N_0+P$ 在 Ω 上等价于 $2M'\sim M_0+M$. 这证明了 M 属于 Ω 当且仅当在 Γ 上有理点 M' 使得 $2M'\sim M_0+M$, 这时 M 对应于 Ω 上的点 $\mu^{-1}(M')$.

对于莫德尔定理 (Mordell's theorem) 的证明, 我们也需要借助于 M 的高 (height)对 M' 的高有一个数量估计, 现将它们的定义叙述于后. 再次令 $M=(x,y)$ 且 $x=X/T^2$, 这里的 X 与 T 互素; 我们定义 M 的高 $h(M)$ 为 $h(M)=\sup(|X|,T^2)$; 类似地, 如果 Ω 上的一个点 N 具有齐次坐标 (U,V,W,T), 它们是没有公因子的有理整数, 那么我们令

$$h(N)=\sup(|U|,|V|,|W|,|T|).$$

如果现在 Γ 的点 M 对应于 Ω 的点 N, 我们则有

$$X=AU^2+\alpha T^2=BV^2+\beta T^2=CW^2+\gamma T^2,$$

因而 U^2, V^2, W^2 有一个依赖于 $|X|$ 和 T^2 的界, 即依赖于 $h(N)$ 的界. 这给出了

$$h(N)\le c\sqrt{hM},$$

其中 c 仅依赖于 Γ. 对于以 $h(N)$ 对 $h(M')$ 进行的估值, 我们可以应用西格尔 (Siegel) 关于高的定理 (参看 C.L.Siegel, *GEd.Abh.*I,249–250, 或者 A.Weil, *Coll. Papers*I.477); 这给出

$$h(M') \leq c'h(N)^{\rho},$$

其中可取 ρ 为任意 $> \frac{1}{2}$ 的数, c' 只依赖于 Ω, M_0 和 ρ. 然而对我们当前的目的而言, 一个较粗的估值就可以了. 像前面一样, 我们有 $M' = \omega_0(N_0, N)$, 从而如果记 $M' = (x', y')$, 则 $x' = \xi(N_0, N)$. 令 $N_0 = (U_0, V_0, W_0, T_0)$; 按定义, $x' = \xi(N_0, N)$ 意味着 $\Phi - x'\Psi$ 在某个点 $(U_0 + tU, V_0 + tV, W_0 + tW, T_0 + tT)$ 等于 0, 其中 $t \neq 0$. 由于 N_0 和 N 满足 $\Phi = \Psi = 0$ 时, 这给出了

$$(5) \qquad x' = \xi(N_0, N) = \frac{\Phi(U_0, V_0, W_0, T_0; U, V, W, T)}{\Psi(U_0, V_0, W_0, T_0; U, V, W, T)},$$

其中分子分母分别是与二次型 Φ 和 Ψ 相关的双线性形式; 它们是 U, V, W, T 的线性形式, 系数只依赖于 Ω 和 M_0. 当然, 对于给定的 M, 这些形式的值不必互素; 但是, 如果我们记 $x' = X'/T'^2$, 其中 X' 与 T' 互素, 则这些值给出了 $|X'|$ 和 T'^2 的上界; 因此我们得到了

$$h(M') \leq c_1 h(N) \leq c_2 \sqrt{h(M)},$$

其中 c_1, 从而 $c_2 = cc_1$ 只依赖于 Γ, Ω 和 M_0.

现在我们回到前面定义的那有限条四次曲线 Ω_i 上; 我们假定在每一条上我们以某种方式选取了一个有理点 N_i; 设 M_i 为它们在 Γ 上的对应点. 对每个有理点 M, 于是必定有一个也只有一个点 M_i 使得 $M + M_i$ 等价于除子 $2M'$, 其中的 M' 是 Γ 的一个有理点. 这里, M 不是唯一决定的; 它可以相差三次曲线 Γ 的有理点群中一个二阶元 (在附录 II 中所解释的意义下); 那些元是无穷远点和三个点 $(\alpha, 0)$, $(\beta, 0)$, $(\gamma, 0)$.

下降法的步骤于是可叙述如下. 以 Γ 的一个有理点 M 为出发点, 我们可在 Γ 上的有理点群的意义下将其写为 $M \sim 2M' - M_i$; 我们有 $h(M') \leq d_i\sqrt{(M)}$, 其中的 d_i 仅依赖于 Γ, Ω_i 和 M_i; 现在可以写成 $M' \sim 2M'' - M_j$, 其中有 $h(M'') \leq d_j\sqrt{h(M')}$, 从而重复这个步骤, 等等. 因此我们得到了点的序列 $M, M', M', \cdots$, 它们的高必定最终小于 m, 这里的 m 取成 $m > \sup(d_i^2)$ 的数. 显然在 Γ 上只有有限多个高不超过 m 的点, 记其为 $P_1, P_2, \cdots, P_r$. 因此, 点 M_i, P_j 生成了 Γ 的有理点群; 这就是莫德尔定理. 原则上, 相同的证明可以应用到 $\mathbb{Q}$ 上有限次扩域为基域的三次曲线上.

出于显然的理由, 上述下降法被称为一个 "对分法" (或 2 分法); 除以任意其他整数原则上也是同样有效的. 尽管除以 2 或 n 的方法被证明对于一般性问

题是最合适的, 但在椭圆函数经典理论中广为人知的是, 除以 n 等价于该曲线函数域的 n^2 次扩张, 它总可以由两个 n 阶的 "变换" (现在叫同源 (isogeny)) 替换. 譬如, 如果我们由 (1) 定义的三次曲线 Γ 着手, 引向四次曲线 $\Omega(A,B,C)$, 于是除以 2 便可通过逐次添加 $u=\sqrt{(x-\alpha)/A}$ 和 $v=\sqrt{(x-\beta)/B}$ 得到, 这里的每一个添加等同于一个二阶的变换. 因此, 对于费马、欧拉和拉格朗日在下降法中使用过的公式相当于这样的变换并不使人感到惊奇 (不包括对曲线 $x^3+y^3=1$ 的处理, 这依赖于三阶的变换; 参看前面的 §16). 在 §17 中我们已经指出, 在拉格朗日关于亏格 1 曲线的主要文章发表大约七年后对 "兰登变换" 的再发现, 可能不仅仅只是个巧合.

现在我们将用处理两个源自费马的例子来解释我们对方程 (1) 的讨论, 这两个例子曾在 §16 中提到过. 首先举出四个平方数构成算术级数的问题; 正如欧拉注意到的, 并在附录 III 中表明的那样, 它等价于方程

$$y^2=x(x+1)(x+4), \tag{6}$$

我们将以前面叙述过的方式来处理它. 按预定的方式, 先从由方程

$$x-Au^2=Bv^2-1=Cw^2-4$$

定义的曲线 $\Omega(A,B,C)$ 中挑出四次曲线 Ω_i; 在此我们必有 $A=bc$, $B=ca$, $C=ab$, 其中 a, b,c 分别除尽 3, 4 和 1; 因此 A 为 ±1 或 ±2, B 为 ±1 或 ±3, 而 $C=AB$. 要是此曲线有实点, C 必须 >0. 考虑同余式

$$AU^2\equiv BV^2-T^2\equiv CW^2-4T^2 \pmod{3^2};$$

如果 (A,B,C) 是 $(2,1,2)$, $(1,3,3)$, $(-1,-1,1)$ 或者 $(-2,-3,6)$, 它们没有被 3 除尽的整数解; 因此这些值应该摒弃. 这样留下了四条曲线 Ω_0, Ω_1, Ω_2, Ω_3, 分别由

$$(A,B,C)=(1,1,1),\ (2,3,6),\ (-1,-3,3),\ (-2,-1,2)$$

给出, 具有分别属于四次曲线 Ω_i 的 Γ 的四个点

$$M_0=\infty,\ M_1=(2,6),\ M_2=(-1,0),\ M_3=(-2,-2).$$

如果令 $P_0=(0,0)$, $P_1=(-4,0)$, 那么在 Γ 的有理点群内二阶元是 M_2, P_0,P_1, 它们连同单位元 $M_0=\infty$ 构成一个四阶群; 容易看出 $2M_1=2M_3=P_0$, $M_1+P_1=M_3$, 所以 $\pm M_1$, $\pm M_3$ 是四阶元.

考虑 Γ 上的实点; 它们构成两条 "分支". 一条 B_0 由 $x\geq0$ 组成并一直延伸到无限远, 另一条是个卵形线 B_1, 由使 $-4\leq x\leq-1$ 的点组成; 在此平面中

的任一条直线必交 B_1 于两个点, 或者根本不交; 按照 Γ 上加法运算的定义, 表明 B_0 是实点群的指数为 2 的子群满足 $B_1 = B_0 + M_2$; B_0 上的每个有理点必定或属于 Ω_0 或属于 Ω_1. 如果这样的点属于 Ω_0 (分别地, Ω_1), 我们可将其写成 $M = 2M'$ (分别地, $M = 2M' - M_1$); 这里, 如果 M' 在 B_1 中, 我们则可将其换作 $M' - M_2$; 因此, 施行下降法, 只要考虑 B_0 上的有理点就可以了.

为了要以前面解释的方式施行下降法, 剩下要做的是得到一个对于 $h(M')$ 的估值, 这个估值当 $M = 2M'$ 或者 $M = 2M' - M_1$ 时要由 $h(M)$ 来表示. 首先假设 M 属于 Ω_0; 用前面一样的记号, 设 $M = (x, y)$ 对应于 Ω_0 上的 $N(U, V, W, T)$; 这里 M_0 对应于 $N_0 = (1, 1, 1, 0)$. 记 $x = X/T^2$ 如上, 以及 $h = h(M) = \sup(X, T^2)$, 我们有

$$X = U^2 = V^2 - T^2 = W^2 - 4T^2,$$

从而

$$|U| \le \sqrt{h},\ |V| \le \sqrt{2h},\ |W| \le \sqrt{5h},\ U \equiv W \pmod 2.$$

至于 M', 它由 (5) 给出; 记 $M' = (x', y')$, $x' = X'/T'^2$, 由于 $U \equiv W \pmod 2$ 我们可将其写成

$$\frac{X'}{T'^2} = \frac{2(V - W)}{\frac{1}{2}(3U - 4V + W)},$$

其中的 X', T'^2 被右端的分子分母所控制. 令 $h' = h(M')$, 我们现在得到

$$h' \le 2(\sqrt{2} + \sqrt{5})\sqrt{h}.$$

相似地, 对于属于 Ω_1 的 M, 以及对于 $M_1 = (2, 6)$, $N_1 = (1, 1, 1, 1)$, 我们有 $h' < 4\sqrt{h}$. 这表明在 Γ 的分支 B_0 上的有理点由 M_1 和高 < 54 的点生成. 至于后者, 设 $M = (x, y)$ 为这样的一个点, 其 $x = X/T^2$; 由于 $x > 0$, 且由于 M 属于 Ω_0 或 Ω_1, 我们有 $X = U^2$ 或 $X = 2U^2$; X 和 T^2 均 < 54. 现在容易验证除了 M_0 和 M_1 外没有其他的这种点. 总结起来, Γ 上仅有 8 个有理点 M_0, M_2, P_0, P_1, $\pm M_1$, $\pm M_3$. 如果现在我们写出四个平方数构成的算术级数:

$$2y^2 = x^2 + z^2,\ 2z^2 = y^2 + t^2,$$

则看出在射影空间 P^3 中它们除了由 $x^2 = y^2 = z^2 = t^2$ 给出的解外再没有其他的了; 这便是费马告诉比利神父的. 另一个例子我们将在附录 V 中论述.

附录 V 方程 $y^2 = x^3 - 2x$

现在我们要把在前面附录 III 和 IV 中所概述的方法应用到费马的问题 (A) 和 (B) 上 (参看前面 §15 和 §16).

我们已经知道, 该问题等同于 §15 中的 "二重方程" (11) 的解, 即方程

(7) $x^2+1=u^2,\ x^2-2x-1=v^2$

的有理数解, 但满足边条件: 在情形 (A) 则 $x>1$, 而在情形 (B) 则 $x<-1$; (7) 定义了一条空间四次曲线 Ω, 它在齐次坐标下可看为由 $\Phi=\Psi=0$ 给出, 其中

(8) $\Phi=X^2-2XT-T^2-V^2,\ \Psi=U^2-X^2-T^2.$

我们可以对它应用附录 III 的结果; 沿用附录的记号, 我们有 $F(\xi)=\xi^3-2\xi$, 而且 Ω 同构于由

(9) $\eta^2=\xi(\xi^2-2)$

定义的三次曲线 Γ.

我们将像附录 IV 中那样进行, 但因为右端的根不全是有理的, 故有些必要的修改. 像附录 IV 中的情形 (6) 那样, Γ 的实点群 Γ_∞ 由两个分支 B_0, B_1 组成, 各自由 $\xi>0$ 和 $\xi\le 0$ 定义; B_0 是个指数为 2 的子群, 并且有 $B_1=B_0+M_2$, 其中 $M_2=(0,0)$; M_2 是 Γ_∞ 的一个二阶元. 如在附录 IV 的情形 (6) 那样, 只要对 B_0 的有理点施行下降法就足够了.

令 $\xi=P/Q$, 其中 P, Q 为互素的正整数; 我们有

$$(Q^2\eta)^2=PQ(P^2-2Q^2)$$

并推断 Q 必为平方数: $Q=V^2$. P 与上式右端第三个因子的 g.c.d. 或为 2 或为 1, 根据 P 为偶或奇而定. 如果 P 为偶, 必有 $P=2U^2$, $P^2-2Q^2=2S^2$, $2U^4-V^4=S^2$. 如果 P 为奇, 我们可将其写成 $P=U^2$, $P^2-2Q^2=S^2$, $U^4-2V^4=S^2$. 顺便说一下, 这个问题因此可化成考虑方程 $2u^4-1=\pm s^2$; 这便是拉格朗日在他 1777 年的文章中如此进行的 (*Lag.*IV,377–398), 在那里他从令 $S=X^2+2XT-T^2$ 开始注意到方程 $\Phi=\Psi=0$ 给出了 $2U^4-V^4=S^2$; 因此在 Ω (或者 Γ) 与四次曲线 $2u^4-1=s^2$ 之间的对应关系是一个二阶变换 ("同源"), 而在 Ω (或者 Γ) 与方程 $2u^4-1=-s^2$ 之间的关系式是相似的.

在这里, 与附录 IV 相类比, 我们将运用对分法与环 $\mathbb{Z}[\sqrt{2}]$, 并沿用附录 I 的记号. 如果 P 为奇数, 令

$$\alpha=P+Q\sqrt{2}=U^2+V^2\sqrt{2};$$

于是 α' 与 α 互素, 并有

$$\alpha\alpha'=N(\alpha)=P^2-2Q^2=S^2.$$

如果 P 为偶数, 令

$$\alpha = Q + \frac{P}{2}\sqrt{2} = V^2 + U^2\sqrt{2};$$

由于 Q 与 P 互素, 它则为奇; 因此 α' 再次与 α 互素, 从而我们有

$$\alpha\alpha' = N(\alpha) = Q^2 - 2\left(\frac{P}{2}\right)^2 = -S^2.$$

在这两种情形, 当把 α 写成在 $\mathbb{Z}[\sqrt{2}]$ 中的素数与单位的积时, 我们发现它是准确到一个单位的平方数, 故它具有形式 $\pm\beta^2$ 或 $\pm\varepsilon\beta^2$, 依 $\alpha\alpha'$ 是 S^2 还是 $-S^2$ 而定; 如前, 这里我们已置 $\varepsilon = 1 + \sqrt{2}$, 且 β 是 $\mathbb{Z}[\sqrt{2}]$ 中的一个整数. 根据上面的公式, 我们有 $\alpha > 0$, 故而一种情形下 α 是 β^2, 而另一种情形则是 $\varepsilon\beta^2$. 令 $\beta = Y - T\sqrt{2}$ 并在上面公式中将 α 替换为 β^2 或 $\varepsilon\beta^2$; 我们得到在一种情形下的

$$U^2 = Y^2 + 2T^2,\ V^2 = -2YT,$$

以及在另一种情形下的

$$U^2 = Y^2 - 2YT + 2T^2,\ V^2 = Y^2 - 4YT + 2T^2.$$

这些成双的方程定义了在射影空间的两条空间四次曲线 Ω_0, Ω_1, 该空间的齐次坐标设为 (Y, T, U, V); 采取与附录 III 一致的符号, 我们令

$$\Phi_0 = 4YT + 2V^2,\ \Psi_0 = Y^2 + 2T^2 - U^2,$$

$$\Phi_1 = Y^2 - 4YT + 2T^2 - V^2,\ \Psi_1 = U^2 - (Y^2 - 2YT + 2T^2),$$

故 Ω_0 (分别地, Ω_1) 由 $\Phi_0 = \Psi_0 = 0$ (分别地, $\Phi_1 = \Psi_1 = 0$) 定义; 不妨注意一下, 替换 $Y = X + T$ 将 Φ_1, Ψ_1 变成了在 (8) 中定义的 Φ, Ψ, 故而 Ω_1 从射影的观点说与 Ω 无异. 再次采用附录 III 的记号, 于是 $F(\xi)$ 对于 Ω_0 为 $4\xi(\xi^2-2)$, 对于 Ω_1 为 $\xi(\xi^2-2)$; Γ 上的点 $M_0 = \infty$, 和 $M_1 = (2, 2)$ 分别属于 Ω_0 和 Ω_1; M_0 对应于 Ω_0 上的 $N_0 = (1, 0, 1, 0)$, 而 M_1 对应于 Ω_1 上的 $N_1 = (1, 0, 1, 1)$; 对于 $i = 0$ 或 1, Γ 上一个有理点 $M = (\xi, \eta)$ 属于 Ω_i 当且仅当存在 Γ 上的一个有理点 $M' = (\xi', \eta')$ 使得 $M \sim 2M' - M_i$. 如果 M 对应于 Ω_i 上的 $N = (Y, T, U, V)$, 则我们有当 $i = 0$ 时的 $\xi = U^2/V^2$, 而当 $i = 1$ 则 $\xi = 2U^2/V^2$. 再次令 $h(M) = \sup(P, Q)$ 以及 $h(N) = \sup(|Y|, |T|, |U|, |V|)$, 在这两种情形都有 $h(N) \leq \sqrt{h(M)}$. 像前面一样, M' 由 $\xi' = \xi(N_i, N)$ 给出, 其中 $\xi(N, N')$ 对于 Ω_i 上任意两点 N, N' 按附录 III 那样定义. 对于 $i = 0$, 由于附录 IV 的 (5), 及 $Y - U$ 必为偶数的事实, 它给出了

$$\xi' = \xi(N_0, N) = \frac{T}{\frac{1}{2}(Y - U)},$$

从而 $h(M') \le h(N) \le \sqrt{h(M)}$. 对于 $i=1$, Y, U, V 必为奇数, 而 T 为偶数; 我们得到

$$\xi' = \xi(N_1, N) = \frac{\frac{1}{2}(Y-2T-V)}{\frac{1}{2}(U-Y+T)},$$

从而 $h(M') \le 2h(N) \le 2\sqrt{h(M)}$. 因此由 Γ 分支 B_0 上的无限下降法产生的序列 $M, M', M', \cdots$ 必定导向一个高 ≤ 4 的点. 因为在 B_0 上这样的点只有 M_1, 这表明 M_1 生成了 B_0 的有理点群; 换句话说, 那些点全由

$$(10) \qquad A_n \sim M_0 + n(M_1 - M_0)$$

给出, 其中 $n \in \mathbb{Z}$, 而那些在 B_1 上的有理点则由

$$(11) \qquad A'_n \sim M_2 + n(M_1 - M_0)$$

给出; 我们于是有 $A_0 = M_0$, $A_1 = M_1$, $A_2 = (9/4, -21/8)$, 等等. 如果 $A_n = (\xi, \eta)$, 则容易看出, 我们有 $A_{-n} = (\xi, -\eta)$ 以及 $A'_n = (-2/\xi, 2\eta/\xi^2)$. 如上所证, 我们有 $h(A_n) \le \sqrt{h(A_{2n})}$, 故点 A_n 的高无界; 这条三次曲线为 "秩 1", 除了显然的等价 $2M_2 \sim 2M_0$ 外不存在 M_0, M_1, M_2 之间的其他等价关系.

现在我们回到费马原来的问题以及由 (7) 定义的曲线 Ω 上. 设 $N = (X, T, U, V)$ 为 Ω 上的一个点; 在 Ω 上取一有理点 P, 譬如 $P = (1, 0, 1, 1)$; 如果像在附录 III 中那样利用它以便得到 Ω 与 Γ 之间的一个同构, 并记 Γ 上对应于 N 的点为 $M = (\xi, \eta)$, 则我们有 $\xi = \xi(P, N)$; 根据附录 IV 的 (5), 并考虑到 (8) 后, 这给出了

$$(12) \qquad \xi = \frac{V - X + T}{X - U} = 2\frac{X + U}{V + X - T}.$$

由此看出 Γ 上对应于 Ω 上的 $N_0 = (1, 0, 1, -1)$ 和 $N_2 = (1, 0, -1, 1)$ 的点分别为 M_0 和 M_2. 至于对应于 $P = (1, 0, 1, 1)$ 的点必定是 $(2, 2)$ 或者 $(2, -2)$, 所以在 Ω 与 Γ 之间的对应中适当地选取 η 的符号后, 我们可假定 $M_1 = (2, 2)$; 因此我们记 N_1 为 P. 于是 Ω 上所有的有理点由类似于 (10) 和 (11) 的公式用 N_0, N_1, N_2 来表出; 看作 Ω 上函数的 ξ 有除子 $2N_2 - 2N_0$. 现在考虑这些平面 $T = 0$, $X + U = 0$, $V + X - T = 0$; 如果令 $N_3 = (1, 0, -1, -1)$, 那么它们在 Ω 上决定了除子

$$\operatorname{div}(T) = \sum_{i=0}^{3} N_i, \ \operatorname{div}(X+U) = 2N_2 + 2N_3,$$

$$\operatorname{div}(X + X - T) = 2N_0 + 2N_3.$$

因此在 Ω 上定义的函数

$$(13) \qquad \zeta = \frac{X+U}{T},\ \theta = \frac{V+X-T}{T}$$

分别具有如下的除子

$$\operatorname{div}(\zeta) = N_2 + N_3 - N_0 - N_1,$$
$$\operatorname{div}(\theta) = N_0 + N_3 - N_1 - N_2.$$

如果 $N = (x,1,u,v)$ 是 Ω 上的一个点, 则具有两个极点 N_0 与 N_1 的函数 $\zeta - (x+u)$ 必定有两个零点, 显然它们是 N 和点 $N' = (x,1,u,-v)$, 故在这种情形下我们有 $N' \sim N_0 + N_1 - N$, 类似地, 利用函数 $\theta - (v+x-1)$, 我们看到, 对于 $N'' = (x,1,-u,v)$ 有 $N'' \sim N_1 + N_2 - N$; 对于 $N'' = (x,1,-u,-v)$ 这给出了

$$N''' \sim N_2 - N_0 + N.$$

特别地, 如果记对应于 Γ 上的点 A_n 为 $B_n = (x_n, 1, u_n, v_n)$, 这表明对应于 A_{1-n} 和对应于 A'_n 的点分别为

$$B_{1-n} = (x_n, 1, u_n, -v_n),\ B'_n = (x_n, 1, -u_n, -v_n).$$

因此这些便是 Ω 上所有的有理点.

我们现在利用这个机会来解释欧拉在其生命后期所引进的一个方法, 即 "提升法" (在 §15 中所使用的字眼的意义下), 用来解亏格 1 的丢番图方程; 这是建立在被他称做 "典则方程 (canonical equation)" (*Eu.*I-5,158 在 E778 中,1780; 参看下文的第三章 §16), 即对 X 和 Y 分别为二次的方程 $F(X,Y)=0$ 的基础上的; 他的方法对于一个稍许不同的但等价于当前问题 (由一对方程 $X+Y=Z^2$, $X^2+Y^2=T^4$ 给出) 的应用可参看 *Eu.*I–5,77–81=E769,1780 以及 *Eu.*I–5,87–88 于 E772,1780 中.

如在前面附录 II 所解释的那样, 欧拉的意义下的一个 "典则方程", 如果在曲线 Ω 上的两个函数中每一个只有两个极点, 则该方程就在这两个函数之间成立. 我们选取同于 (12) 和 (13) 定义的 ξ 和 η 为这些函数. 如前, 令 $x = X/T$, $u = U/T$, $v = V/T$, 有 $x + u = \zeta$, 并且, 根据关系 $x^2 - u^2 = -1$, 有 $x - u = -1/\zeta$; 这给出了

$$x = \frac{1}{2}\left(\zeta - \frac{1}{\zeta}\right), \qquad u = \frac{1}{2}\left(\zeta + \frac{1}{\zeta}\right).$$

与此同时, 公式 (12) 给出了

$$v - x + 1 = \xi(x-u) = -\frac{\xi}{\zeta}, \quad v + x - 1 = \frac{2}{\xi}(x+u) = \frac{2\zeta}{\xi},$$

从而

$$v = \frac{\zeta}{\xi} - \frac{\xi}{2\zeta}, \qquad x - 1 = \frac{\zeta}{\xi} + \frac{\xi}{2\zeta}.$$

比较上面所得到的 x 的值, 我们有了 ξ 与 ζ 之间的一个关系式, 它可写成一个"典则方程"

$$F(\xi,\zeta) = \xi\zeta^2 - \xi^2 - 2\xi\zeta - 2\zeta^2 - \xi = 0.$$

另外, 上面的公式决定了一个双有理对应, 即在 Ω (或者等同于在 Γ) 和由 $F = 0$ 定义的平面曲线 C 之间的一个同构; C 上对应于 N_0, N_1, N_2, N_3 的点分别为

$$P_0 = (\infty,\infty),\ P_1 = (2,\infty),\ P_2 = (0,0),\ P_3 = (-1,0).$$

应用于方程 $F = 0$ 的欧拉的 "提升法" 现可表达如下. 设 $R_0 = (\xi_0,\zeta_0)$ 为 C 上的任一有理点; 由于 F 对 ζ 的次数为 2, 方程 $F(\xi_0,z) = 0$ 除 ζ_0 外有第二个有理根 ζ_1, 它由

$$\zeta_1 = \frac{2\xi_0}{\xi_0 - 2} - \zeta_0 = -\frac{\xi_0(\xi_0+1)}{\zeta_0(\xi_0 - 2)}$$

给出; 这决定了 C 上的一个点 $S_0 = (\xi_0,\zeta_1)$; 函数 $\xi - \xi_0$ 的除子于是为 $R_0 + S_0 - 2P_0$, 故我们有

$$S_0 \sim 2P_0 - R_0.$$

类似地, 方程 $F(x,\zeta_1) = 0$ 有第二个解 ξ_1 , 由

$$\xi_1 = \zeta_1^2 - 2\zeta_1 - 1 - \xi_0 = \frac{2\zeta_1^2}{\xi_0}$$

给出, 并决定了 C 上一个点 $R_1 = (\xi_1,\zeta_1)$, 对此我们有

$$R_1 \sim P_0 + P_1 - S_0.$$

重复着同一步骤, 我们得到了一系列的 R_0, S_0, R_1, S_1, 等等, 用归纳容易给出

$$R_n \sim R_0 + n(P_1 - P_0), \quad S_n \sim 2P_0 - R_n.$$

如果我们取, 譬如, 点 $R_0 = P_0$ 为初始点, 与上面得到的公式的比较表明 R_n, S_n 是那些在 C 上分别对应了 Γ 上的 A_n, A_{-n} 的点. 在这种情形我们有 $R_0 = S_0 = P_0$, $R_1 = P_1$, $S_1 = (2,-3/2)$, 于是利用上面的公式有:

$$R_2 = \left(\frac{9}{4},-\frac{3}{2}\right), \qquad S_2 = \left(\frac{9}{4},\frac{39}{2}\right),$$

$$R_3 = \left(338,\frac{39}{2}\right), \qquad S_3 = \left(338,-\frac{1469}{84}\right),$$

$$R_4 = \left(\frac{12769}{7056},-\frac{1469}{84}\right), \quad S_4 = \left(\frac{12769}{7056},-\frac{172325}{112812}\right),$$

等等.

于是 Ω 上的点 $B_n = (x_n, 1, u_n, v_n)$ 是由上面公式对应于 R_n 的点, 而 $(x_n, 1, \pm u_n, \pm v_n)$, $n = 0, 1, 2, \cdots$ 为 Ω 上所有的有理点. 特别地,(除 $x_0 = x_1 = \infty$ 外, 它们分别对应于 Ω 上的 N_0, N_1) 我们有

$$x_2 = -\frac{5}{12},\ x_3 = \frac{1517}{156},\ x_4 = -\frac{2150905}{246792},$$

$$x_5 = -\frac{16969358281}{38880655800}.$$

费马的问题 (A) 要求有一个满足 $x > 1$ 的解; 问题 (B) 要求 $x < -1$; 他的解确实是最小的可能解, 分别对应了 x_3 和 x_4.



老年的欧拉

第三章　欧拉

§3.1　十六世纪、十七世纪和十八世纪的科学活动

直到十七世纪后期, 数学才间或使它的专家们获得高度的声誉, 但却极少能给予他们社会生活的提升和受尊崇的职业. 韦达靠律师维持生计, 费马是个地方官员; 甚至在费马的年代, 给予数学的位置非常稀少. 在意大利, 闻名整个欧洲的博洛尼亚大学 (通常称为 "*lo studio di Bologna*") 的确在十六世纪初把费罗*1列入了他们的教授之中; 但是卡尔达诺*2 是个活跃的医生; 邦贝利是个工程师, 荷兰的西蒙・史提芬也是个工程师, 对数发明人纳皮尔 (Napier) 则是个苏格兰的领主, 从早年的游历返回后一直居住在他的曼彻斯顿的古堡里. 相邻学科的遭遇也好不到哪里去. 哥白尼是个教会的显要. 开普勒 (Kepler) 的老师梅斯特林 (Maestlin) 是图宾根大学的教授, 但开普勒从事的行业则是占星家和天宫图制作者. 伽利略的天才加上他的霸气的个性为他赢得了帕多瓦的教授职位, 而后则是令人羡慕的、托斯卡纳区大公的被保护人的地位, 这使他避免了与罗马教廷冲突的灾难性后果; 他的学生托里拆利继承他作为大公的 "哲学家和数学家", 而卡瓦列里则身兼博洛尼亚大学教职与同城的 Gesuati 女修道院副院长.

在与费马进行科学方面的通信者中, 很少具有专业职衔的. 罗伯瓦尔就职于法兰西学院 (*Collège de France*) (后来称作皇家学院), 占有设立于 1572 年的教授职位, 该职位是科学家、哲学家皮埃尔・拉梅 (Pierre Ramée) 的遗赠. 由 H.

---

*1Scipione del Ferro, 1465—1526, 意大利数学家, 因发现三次方程解公式而知名.

*2Cardano 1501—1576, 意大利数学家, 著有《大衍术 (*Ars Magna*)》. 他有多方面的才干, 曾写过一本概率对局的书, 这是有关概率论最早的一本书.

布里格斯*3 于 1620 年在牛津大学设立的 Savilian 教席被沃利斯从 1649 年直至他逝世的 1703 年所据有; 但是他的天才的年轻朋友与合作者威廉 · 布龙克尔子爵二世是个贵族, 其职业是个海军专员, 他的恋情还被佩皮斯*4记载在他的日记中. 只是到了 1663 年巴罗*5才成为剑桥的第一任卢卡斯教授, 他于 1669 年放弃了该职位而由牛顿继任, 他转而成为查理二世的传教士, 并取得了作为牧师的高声誉. 在荷兰, 虽然笛卡儿的朋友、评论家舒腾是莱顿大学的教授, 但斯路思 (René de Sluse)却被认为是在当代人中具有高度评价的数学家、一位具有魅力个性的人, 而他是在 Liège 的一个教士. 笛卡儿, 如他所告诉我们的, 觉得他自己受到上帝的恩宠 (“*graces à Dieu*”: 《方法论 (*Discours de la Méthode*)》, *Desc.*VI9), 超越于为利的职业; 他的朋友康斯坦丁 · 惠更斯, 和他的儿子伟大的克里斯提 · 惠更斯也是如此. 莱布尼茨则服务于汉诺威法庭; 他终身保持着对数学的挚爱, 然而他的朋友们时时对他的职业居然留给他足够的闲暇来与他们交流感到惊讶.

不管他们有什么职业, 这些人对于数学的态度常常能将其描述为彻底职业化的. 不管是通过发表文章还是通过信件, 它们总是不懈地转播他们的思想和结果并保持与当代的进展同步; 为此他们在很大程度上依赖于一个私人的信息网. 当他们旅行时便去拜访国外科学家. 在国内他们则接待以科学为目的的旅行者, 像是一些蜜蜂专心地散播着从各处采集来的花粉. 他们渴望寻找与自己兴趣相似的通信者; 信件从这个人传到那个人直到到达那个感到关切的某人手中. 一个适当规模的私人图书馆几乎是必须的. 书商有常备的订单以提供顾客各自选择领域的最新出版物. 这个体系, 或者缺少系统, 却十分良好地运行着; 是的, 它一直维持到当今, 作为对更加正式的交流模式的补充, 而价值并未消失. 但是, 甚至在十七世纪必定也发现了它日益增大的缺陷.

在欧拉诞生的 1707 年, 发生了一个根本性的变化; 它的第一个信号甚至在费马逝世前就已明确显示出来了.《*Journal des Sçavans*》*6于 1665 年创刊, 正好及时地发布了关于费马的讣告 (在那里称他是 “伟大的人” (*ce grand homme*)). 路易十四的有远见卓识的大臣柯尔贝尔 1666 年把惠更斯吸引到了巴黎, 又在 1669 年将天文学家卡西尼 (Cassini) 吸引到巴黎, 授予每人一笔王室奖金, 这类奖迄今仍保留在文学类上. 1635 年黎塞留*7创建了法兰西研究院 (*Académie françoise*); 更具实践思想的柯尔贝尔意识到科学研究 (纯粹的与应用的相同) 对

---

*3H. Briggs, 1561—1630?, 英国数学家, 以发明常用对数, 制定对数表闻名.

*4S. Pepys, 1633—1703, 英国文学家, 海军行政长官, 以其记载了王政复辟, 鼠疫和伦敦大火的日记而闻名.

*5Issac Barrow, 1630—1677, 牛顿的老师, 微积分学的先驱者, 发现微积分基本定理.

*6该杂志由 Denis de Sallo 创建, 是欧洲最早的一份科学方面的杂志.

*7Due de Richelieu, 1585—1642, 路易十三的国务秘书兼御前会议主席, 当时的强势人物.

于整个王国昌盛的价值, 于 1666 年建立了围绕着大体上是费马的前信友组成中心的科学院 (*Académie des sciences*); 费马的伟大朋友和前同僚卡尔卡维被委以行政事务, 并成为第一任秘书. 在英格兰, 由于查理二世的返国, 1660 年恢复了某种程度上的政治稳定; 1662 年, 在格雷欣学院 (*Gresham College*) 里举行了一段时间正规会议的业余爱好者 ("*virtuosi*") 团体收到了一份让他们组成皇家协会 (*Royal Society*) 的宪章, 并以布龙克尔为其第一任主席; 1665 年他们开始出版《哲学学报 (*Philosophical Transactions*)》, 它一直延续到了今天. 1698 年法兰西研究院连续不断地出了一系列的年度刊物, 形形色色地冠以*历史* (*Histoire*) 和*科研论文集* (*Mémoires de l'Académie des Sciences*). 1682 年, 莱布尼茨在创建虽然说不上是个研究院但至少是一份主要科学杂志中起了推动作用, 这份杂志是在莱比锡的《*Acta Eruditorum*》, 他在其最初几期上发表过文章, 它们产生出了微积分 (infinitesimal calculus).

很快, 各个大学和研究院为得到科学人才而竞争, 并不惜人力和财力来吸引他们. 雅各布 · 伯努利 (Jacob Bernoulli) 于 1687 年在他家乡城市巴塞尔成了一名教授; 只要他一息尚存, 那么留给他的弟弟也是他的厉害的竞争对手约翰在那里找到一份研究职位的前景就十分渺茫; 约翰先是教给一位法国的贵族洛必达 (Marquis de l'Hôpital) 莱布尼茨微积分, 甚至同意了一份不平常的合同, 使后者对于伯努利的所有数学发现具有优先权. 然而在 1695 年, 约翰 · 伯努利以十分有技巧地在乌得勒支大学和格罗宁根大学间的竞争, 取得了格罗宁根的教授职位, 从而改变了他的境遇; 最终在他的兄长逝世后, 于 1705 年定居在了巴塞尔. 那么, 当我们发现在 1741 年他祝贺欧拉的柏林任职带来的 (适当的年俸, "*pro modico subsidio annuo*": *Corr.* II, 62) 金钱方面的好处, 并且同时提出他愿意以自己的贡献使柏林科学院的科研文集更加丰富时, 我们并不感到惊奇. 简短说来, 在世纪更迭时期的科学活动所获得的结构与我们今天所证实的没有太大的差别.

§3.2 欧拉的生平

欧拉的父亲保罗 · 欧拉是一个靠近巴塞尔的 Riehen 中所建教区的牧师; 他在巴塞尔大学学习了神学, 同时参加了雅各布 · 伯努利的讲座; 他给他的儿子设计了相似的事业道路, 但当年轻的列昂哈德的爱好已显露无遗时, 他并没有设置任何障碍. 毫无疑义, 在那个时候, 对于任何具有特殊科学天分的年轻人来说光辉的未来在等着他们.

1707 年当欧拉诞生之时, 雅各布 · 伯努利死了, 约翰 · 伯努利则继承了他; 约翰的两个儿子尼古拉斯 (生于 1695 年) 和丹尼尔 (生于 1700 年) 继承了家族

的传统, 但相对照于他们的父亲和伯父, 他们却非常相亲相爱, 因为他们尽力相互了解 (譬如参看 *Corr.*II,291). 欧拉成了他们的亲密朋友, 并成了约翰宠爱的门生; 在欧拉老年之时, 他喜欢回忆起他是怎样每个星期六拜见他的老师的, 并且把在这一周里遇到的困难搁在他的面前, 还有是如何努力工作以便不要以不必要的问题去麻烦他.

在欧拉的事业中三位君主起了决定性的作用: 彼得大帝, 腓特烈大帝, 叶卡捷琳娜女皇. 彼得, 或许是真正伟大的沙皇, 死于 1725 年; 但他已有时间去建立圣彼得堡, 竖立起了它的一些最令人印象深刻的建筑, 而对我们的故事而言最重要的是做出了科学院的计划, 这个科学院是按照他在西方所见到的模式来规划的; 那些计划由他的遗孀忠实地执行了. 1725 年两个年轻的伯努利——尼古拉斯和丹尼尔, 被召唤到此. 尼古拉斯在第二年就亡故了, 显然死于盲肠炎. 大约在同一时间, 一份到圣彼得堡科学院任职的提议给了欧拉. 他那时还没有完全满二十岁; 而他刚好有一篇关于船舶建造的获奖论文, 其实在他的现实生活中还从来没有见到过出海的船只. 在国内他并没有什么预先的期待. 他爽快地接受了邀请.

他从巴塞尔沿莱茵河顺流航行到美茵茨, 然后穿越到吕贝克, 大部分是步行, 途中拜访了克里斯廷 · 沃尔夫 (Christian Wolff), 他是一位哲学家, 莱布尼茨的追随者, 被一个不懂哲学的国王从柏林流放至此 (他是如此告诉欧拉的). 他反复唠叨的话题是莱布尼茨的单子学说, 而欧拉显然对此没有什么印象. 从吕贝克出发的一艘船载着这位年轻的数学家驶向了彼得堡.

在那些日子里, 学术单位都是些先天条件甚厚的研究机构, 提供了丰富的资金和优良的图书馆 (参看 *Corr.*I,36). 它们的成员享有相当大的自由度; 他们首要的职责就是实质性地贡献学术的出版物并在国际科学界保持其崇高的声誉. 同时, 他们也是君主们和政府当局的科学顾问, 当这些人觉得他们适合于一项任务时就会指派给他们, 而他们总是随时准备着接受这些任务, 不管适宜与否. 正如欧拉曾经向叶卡捷琳娜承认的那样, 如果不去这样做, 没有一个政府会容忍为维持这种机构所付出的高昂费用 (参看 *Eu.*IV A-1, no.1887; 1766). 1758 年, 在其名望甚高之时, 欧拉 (他在彼得堡已熟练地掌握了俄语) 曾为腓特烈国王翻译过的一些急件在与俄军的军事行动中被俄方截获; 而他既没有觉得这会降低他的身份, 也没有觉得与彼得堡科学院保持紧密关系会产生不协调.

然而在 1727 年当欧拉到达彼得堡时, 政治局势已经改变. 在一位新沙皇下所有科学院的任命全都终止待定. 在欧拉获奖文章的影响力下, 他被委任到海军任职, 但没有在那里呆多久. 很快他就成了科学院的一名有薪酬的成员, 起初是个职位较低的 "助理". 当他的朋友丹尼尔 1733 年离开到巴塞尔时, 他被任命到丹尼尔的职位上; 这样他便能够结得起婚, 自然是与当地的一个瑞士侨民家族

联姻, 另外还给自己买了一座舒适的房子 (参看他 1734 年给同事 G.F.Müller 的信; *Eu*.A-1,no.1683). 他的新娘是一位画家 Gsell的女儿; 在以后的时间中她生了十三个孩子, 其中只给欧拉存活了三个儿子; 除此之外, 关于她几乎没有其他的记载. 大儿子约翰 · 阿尔伯特生于 1734 年, 注定成为了他父亲的一个合作者, 后来则是这个科学院的一个领导成员.

尽管由于丹尼尔的离开留给他了一个相对孤立的状态, 然而一旦欧拉在彼得堡很好地定居下来了, 他的成果远远超出了所有的预期. 即便在 1735 年的一场严重的疾病以及后来的失去右眼也几乎没有使他中断. 他毫无疑义地是该科学院里最有价值的成员, 并且当在欧洲政治的上层中的两大事件带给他的平静生活重大变化时, 他的声望却得到了跳跃式地增长. 在彼得堡 1740 年女沙皇的逝世, 一个摄政政权, 以及紧接着的骚乱, 似乎威胁到了科学院的生存. 正好在此关头, 腓特烈大帝继任了他父亲 (就是那个曾将沃尔夫傲慢地驱出出柏林的皇帝) 的普鲁士王位; 他立即采取步骤直接要求建立一个在他保护下的科学院, 为此他查遍了欧洲科学界最著名的名字, 自然欧拉名列其中. 腓特烈给了欧拉一份慷慨的任职邀请, 加之彼得堡急剧恶化的局势, 经过在波罗的海上三个星期的航行, 其间除了他自己外 (据他自己所声称的) 整个家庭成员都遭受到晕船之苦, 他终于在 1741 年 7 月到了柏林 (参看他在 1741 年 8 月 1 日给哥德巴赫的信: L. Euler and Chr. Goldbach,《*Briefwechsel*》edd. A.P. Juškevič und E. Winter, Berlin 1965,p.83). 再接下来使他极其满意的一年中, 他购买了一座极好的房子, 位置也佳, 并由王室下令免于征用 (索引同上,p.130, 1742 年 12 月 15 日). 再后来的 24 年里他一直住在这里, 显然只有对他乡下地产的季节性造访以及在 1750 年全家到法兰克福的旅行去迎接从巴塞尔来到柏林与他同住的寡居的母亲才造成仅有的中断; 那个乡下的不动产是他于 1752 年在查尔罗滕堡取得的 (参看 *Eu*.IVA-1,no.2782), 而想要欧拉造访巴塞尔的希望落空了的 (参看 *Corr*.II,57,451) 他的父亲于 1745 年与世长辞.

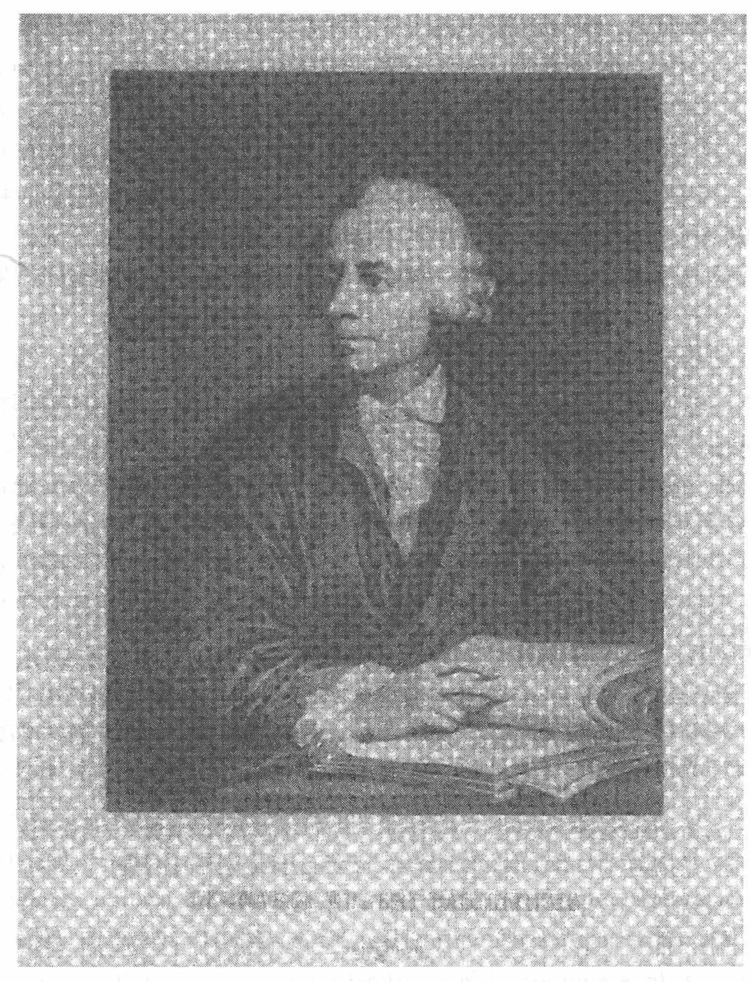
人们或许以为随着欧拉居住地的改变, 他的源源不断发表的文章会从彼得堡转到柏林; 但远非如此! 它不仅被允许保留他的彼得堡科学院院士资格, 而且他在彼得堡的年金仍旧继续, 他一心要向他过去的同事们表明他们金钱的价值 (譬如参看 *Corr*.I,200;1743). 他的曾外孙 P-H. Fuss可能很贴切地描述欧拉的柏林期间为 "25 年不可思议的活动". 给彼得堡送去超过 100 篇的专题研究报告, 127 篇在柏林发表的有关在纯粹和应用数学中所有可能的课题都是那些年代中的成品, 与主要关于分析的论文一起的, 还有关于火炮学的, 船舶建造的, 月球理论的; 更不用说那些送交巴黎科学院的获奖论文了 (除了高荣誉外它的奖金也带来了实质的金钱回报; 参看 *Corr*.I,497;1749); 人们对此还必须加上《给一位德国公主的信》(曾经有过的最成功的科学通俗读物之一:*Eu*.III-11 以

及 III-12=E343,344;1760–1761), 甚至还有一篇对基督教的辩护文 (*Rettung der göttlichen Offenbarung...,Eu.* III-12, 267–286=E 92;1747), 它对原作者没有一点曲意奉承, 而该作者就是自充的哲学家 —— 腓特烈国王. 与此同时, 欧拉有了日益沉重的通信负担, 有科学方面的, 私人的, 也有官方的, 因为科学院的行政担子越来越多地压在了他的肩上.

随着岁月流逝, 欧拉与腓特烈已不再相互着迷了. 国王不再去留意欧拉投射到他的科学院上的光彩了, 但是法国文学界在他的所爱中处于远为高大的地位. 他在寻求吸引达朗贝尔到柏林来的机会并期望将他置于欧拉之上做所谓科学院的头 (参看 *Corr.*I,667,668,670,672;1763). 欧拉幸免了这个对于自尊心的打击; 达朗贝尔或许得到了伏尔泰与腓特烈在 1753 年的不愉快经历的事先警告, 在一段短时间访问中享受了国王宠爱的舒适和温暖, 但他对于自由的评价远远高于更长久地疏远它. 然而, 早在 1763 年欧拉就已萌生了重新返回俄罗斯的想法.

幸运的是, 在那里恰恰发生了另一件政治剧变. 1762 年沙皇的德国妻子在自己和俄罗斯摆脱了她的丈夫后作为叶卡捷琳娜二世掌了大权. 她的首要计划之一便是恢复彼得堡科学院昔日的光辉. 这几乎就是召回欧拉的同义词. 谈判拖延了三年. 终于在 1766 年, 俄国驻柏林的大使奉命请求欧拉写出他自己的合同. 很晚才意识到这个巨大损失的腓特烈试图在其中设置障碍; 他很快发现负不起冒犯这个女皇帝的责任. 同年, 欧拉在通过波兰的凯旋之旅后回到了彼得堡, 在波兰叶卡捷琳娜的前情人, 斯坦尼斯拉斯 (Stanislas) 接待他就几乎像是他的同伴君主那样.

之后欧拉失明了. 在第一次逗留彼得堡期间他已不能用他的右眼了. 大约在他离开柏林这个时间或稍后一些, 在他的左眼白内障有所发展. 1770 年在回复拉格朗日关于数论的信中他描述了他的状况如下: “ *Je me suis fait lire toutes les opérations que vous avez faites sur la formule* 101 = *pp* − 13*qq et je suis entièrement convaincu de leur solidité; mais, étant hors d'état de lire ou d'écrire moi-même, je dois vous avouer que mon imagination n'a pas été capable de saisir le fondement de toutes les déductions que vous avez été obligé de faire et encore moins de fixer dans mon esprit la signification de toutes les lettres que vous y avez introduites . Il est bien vrai que de semblables recherches ont fait autrefois mes délices et m'ont coûté bien du tems; mais à présent je ne saurois plus entreprendre que celles que je suis capable de dévellopper dans ma tête et souvent je suis obligé de recourir à un ami pour exécuter les calculs que mon imagination projette* ” [“我已将您所有关于方程 $101 = p^2 - 13q^2$ 的计算叫人读给我了, 我完全相信它们的正确性; 但是由于不能读和写, 我必须承认我的想象还跟不上您所采取的所有步



中年的欧拉

骤的推理, 也不能记住您所有记号的意义. 的确, 这样的一些研究曾带给我一种愉悦并且为它们花费了许多时间; 但是现在我只能从事那些可以在我头脑中进行的东西, 我常常不得不依靠某个朋友来做我已想好了的计算"; *Eu.*IV,A-5,477, 1770 年 3 月 9 日].

在 1771 年欧拉做了一个手术, 起初是成功的, 但不久眼睛受到了感染, 随后完全或者说几乎完全瞎了. 除了这个不幸外还有在彼得堡的一场大火, 他的房子也被烧毁; 他的生活过得舒适, 非常荣耀, 受人尊敬; 不管是老龄还是失明都不能促使他享用完全应得的休息. 他有助手, 其中一个是他的儿子, 其他一些人是在他的老朋友丹尼尔 · 伯努利的协助下从巴塞尔来的; 我们还应该感谢其中的一个人 N. Fuss, 他于 1773 年来到彼得堡, 后来与欧拉的一个孙女结婚, 就是他对于欧拉在其生命的最后十余年的研究方法给了生动的描述 (*Corr.*I, XLIV–XLV). 在此期间写出了成百的研究报告; 如欧拉所预言的, 足以塞满今后许多年的科学院的刊物了. 他在 1783 年 9 月 18 日突然撒手人寰, 就在最后这一天, 他还一直保持着极好的整体健康状况和充沛的精神活力.

§3.3 欧拉与哥德巴赫

没有一个数学家像欧拉在十八世纪的最合适时间中所做过的那样, 在数学的不管是纯粹的还是应用的所有分支中, 达到了一个无可争议的领导地位. 在 1745 年他的老迈的、通常并非一个谦虚者的老师约翰 · 伯努利, 称呼他为 "数学王子 (*mathematicorum princeps*)" (*Corr.*II,88,92). 达朗贝尔则是以一种可笑的厌恶态度评价他是 "有魔力的人 (*Ce diable d'homme*)". 这是达朗贝尔 1769 年写信给拉格朗日时说的, 他发现他自己陷进了自己引以为骄傲的一些结果中, 而这却是早在欧拉的预料之中的 (*Lag.*XIII,136).

在这里我们关心的是他在数论方面的工作, 即便他没有做其他什么, 就单单这一项已为他赢得了数学史上的一个卓著的地位; 然而这只占他七十多卷全集中的四卷. 他似乎间歇性地以此为首要研究对象. 或许在他作为约翰 · 伯努利的徒弟时对此还没有充分准备好, 但在其职业生涯中的早期就已从事了这项研究, 并且它一直到生命的尽头都是他钟爱的课题. 他充分了解, 这个课题对他的同代人而言已不再像在十七世纪中那样受欢迎了 (参看第二章 §17; 也可参看下面 §10 所引的丹尼尔 · 伯努利对于素数课题的轻蔑评注). 但是欧拉孜孜不倦地告诉他的读者说, 他感到没有必要为此所耗费的时间和精力而抱憾, 真理是统一的, 不可能它的一个方面受到忽视而不伤害到整体 (参看, 譬如,*Eu.*I-2,62–64,295,428,461–462,519–522, 等).

欧拉在算术方面工作的实质部分只是、也正好是对费马在他那时发表了的

著述中的陈述给出证明 (参看下文的 §4). 我们在前面第二章中对费马原来证明的尝试性重建, 大体上是建立在看起来正确却并没有得到证实的假设基础上的, 这个假设是说, 这些证明与那些后来由欧拉得到的证明相距不远. 因此在这里便没有必要把这些证明详细重述了; 只要把欧拉的这些发现按编年简要说明就够了. 除了他对彼得堡科学院的学术报告的提交日期有时会与它们发表的日期相差许多年外, 对此的一个重要来源是他的通信, 首要的是与哥德巴赫的通信, 他在 1843 年由欧拉的曾外孙 P-H. Fuss 出版; 它构成了《物理与数学通信 (*Correspondance Mathématique et Physique*)》(*Corr.*I) 的第一卷; 第二卷包含了由伯努利们给欧拉、哥德巴赫和 N. Fuss 的信件; 哥德巴赫关于素数和的猜想就出现在那里的哥德巴赫的 1742 年 6 月 7 日的信中 (*Corr.*I,127). 一本对此同样的通信但却更完整的富于注释的书则属于 A.P. Juškevič 和E. Winter (参看本书后面的参考书目). 在欧拉与伯努利之间更多的信件包含在 1862 年欧拉的《遗作 (*Opera Postuma*)》中 (vol.I, pp,519–588) 和在从 1903 年到 1907 年的 *Bibl.Math.* 的 G.Eneström 的文章中 (参看参考书目). 欧拉与克莱罗、达朗贝尔以及拉格朗日的信件已以*Eu.*IV A-5 完整形式出版; 还有与各种同代人的通信 (以原始文本和俄文译文) 构成了一卷《*Pis'ma k Učënym*》, Moskva–Leningrad 1963 (*PkU.*); *Eu.*IV A-1 是欧拉浩大信件的一个完整的贮藏库, 并附有简短提要. 只要是涉及数论的, 至少是从 1730 年到 1756 年的, 一定可以在他给哥德巴赫的信中找到.

哥德巴赫于 1690 年生在柯尼斯堡 (Königsberg); 是一个多才多艺、具鉴赏力、有才干的男子汉, 显然有良好教养, 并且富有, 在他年轻时旅行过广阔的地区 (参看 *Corr.*II,183–184), 到各处寻访饱学之士和科学家. 1721 年他在威尼斯遇到了尼古拉斯 · 伯努利; 之后不久就开始与他通信, 而后也与其弟丹尼尔通信. 在 1725 年在将他们两人带到彼得堡的事上他起了很大的作用, 他比这两兄弟早到那里几个月 (参看 *Corr.*II,169); 他似乎被这两兄弟, 还有很快以后的欧拉, 视为有影响力的朋友和保护人; 终其一生欧拉一直以一种混合了重视、敬重和友爱的令人感动的方式对待他. 或许哥德巴赫最初踏上去俄罗斯之路仅仅出于好奇; 但直到 1764 年逝世他一直留在了那里, 时而在彼得堡时而在莫斯科; 他首要的业余爱好是语言和数学, 更特别是数论、微积分和级数理论; 这使得他成了欧拉的一位极其宝贵的通信者.

哥德巴赫在 1728 年离开彼得堡到了莫斯科; 他与欧拉的通信开始于 1729 年; 最初完全使用拉丁文, 甚至在 1732 年哥德巴赫回到彼得堡后仍然继续, 当然不怎么频繁, 在那时他们几乎每一天都必须要见到对方. 突然, 在 1740 年 8 月 1 日欧拉不知不觉地用德语写下了一个请求帮助的紧急请求 ("*Die Geographie ist mir fatal*(地理对我来说是要命的)", *Corr.*I,102; 当他想到因制图工作已丢掉了一只眼, 他现在要求不再被分派去做类似的工作, 这不仅与他正规的职责背道而

驰, 而且对他的视力的威胁是毁灭性的. 哥德巴赫公正地给了警告, 并在这同一天给了欧拉回信, 也是用的德文. 在接下来的几年, 欧拉到了柏林, 通信不断地继续着, 基本上用德语, 直到接近哥德巴赫生命的尽头才停止. 然而他们的德语不仅点缀着法语词汇, 而且往往写下了拉丁文, 特别在数学的行文中. 这里是一个样本, 取自欧拉到达柏林后的第一封信 (*Corr.*I,105–107,1741 年 9 月 9 日); 在介绍了国王和皇族给予他的亲切接见和其他各种事情之后, 欧拉对他关于数论和 "欧拉积分" 最新想法进行了叙述:"*Von den divisoribus quantitatis* $aa \pm mbb$, *si a et b sint numeri inter se primi, habe ich auch curieuse proprietates entdeckt, welche etwas in recessu zu haben scheinen...*" ["关于 $a^2 \pm mb^2$ 的因子, 如果 a 和 b 互素, 我已发现了一些令人好奇的性质, 那里似乎隐藏着一些秘密······"]. 这里的 "令人好奇的性质 (*curieuse proprietates*)" 是用拉丁文写的 (参看下文的 §6 和 §8).

§3.4 欧拉关于数论的发现

就是在哥德巴赫回复欧拉给他的第一封信中, 数论露了一下脸. 在 1729 年 10 月 13 日, 欧拉在丹尼尔的建议下, 寄给哥德巴赫他的一些早期的结果, 这是些关于自勒让德后被称为的 Γ 函数 (*Corr.*I,3–7); 显然他一直在读沃利斯的《无穷的算术 (*Arithmetica Infinitorum*)》(*Wal.*I,355–478). 在 12 月 1 日哥德巴赫给了一个热忱的、足够适当的回答, 没有说出什么新的东西; 但是它传送了一个带有宿命色彩的附言:"您知道费马的评述, 说所有数 $2^{2^n}+1$ 都是素数吗? 他说他不能证明它; 就我所知也没有任何其他人做到了这点" (*Corr.*I,10).

实际上哥德巴赫从没有读过费马的东西 (稍后他向欧拉如是说:*Corr.*I,26) 是从传闻引述的; 对于在他信中其他提到费马的也同样如此 (譬如 *Corr.*II,168, 238;1725). 费马的断言在 "数的爱好者" 中作为一种民间传说传播着; 欧拉称它们为 "众所周知" ("*in vulgus notas*":*Eu.*I-2,38 于 E98 中;1738).

欧拉对于哥德巴赫的问题回应多少有点冷谈, 仅仅表达了怀疑 (*Corr.*I,18). 但是哥德巴赫仍在坚持 (*Corr.*I,120), 在 1730 年, 欧拉突然热情迸发. 不仅他现在认真对待这件事了, 而且已经拿起了费马的著作, 开始读了起来 (*Corr.*I,24).

人们会问, 他那时不知有哪些费马的著述容易得到. 这些有 1679 年的《*Varia Opera*》和 1658 年的《*Commercium Epistolicum*》(包含了费马写的一些重要的信件), 沃利斯曾把它放进他 1693 年的具有纪念碑意义的《代数》里; 欧拉在 1732 年都引用了这两本书 (*Eu.*I-2,2 于 E26 中). 是否他也得到在塞缪尔 · 费马 1670 年所编《丢番图》(参看第二章 §1) 中费马的评述? 到 1748 年之前他一直没有提到过它们, 但之后他三次引用过它们, 在写给哥德巴赫的信 (*Corr.*I,455;1748) 中,

他第一次提到了关于"费马方程" $x^n+y^n=z^n$ 的费马评述 (*Fe*.I,291,Obs.II); 而后在下一封信 (*Corr*.I,155;1748) 中, 他完整地抄写关于四平方和的评述, 等等, 并谈到费马打算要写整本关于这个主题的书的事 (*Fe*.I,305,Obs. XVIII); 同年他写了一篇文章 (*Eu*.I-2,223–240=E167;1748), 专门讨论费马在《丢番图》中陈述的丢番图问题 (*Fe*.I,333,Obs.XL). 难道这看起来不像是欧拉在那个时候刚刚才发现了费马的《丢番图》吗?

无论怎样, 当欧拉在 1730 年拿起费马的著述时, 他在那里发现了一个陈述 (显然是费马给迪格比的一封信中的,《通报 (*Commercium Epistolicum*)》no. XLVII; *Fe*.II,403), 该陈述给了他深刻的印象, 甚至比关于 $2^{2^n}+1$ 的猜想还要深, 就正像当它第一次出现时给惠更斯的印象一样 (参看第二章 §17). 当他告诉哥德巴赫说, 费马说过每个数都是四个平方数之和 (欧拉有点不合适地称其为"*non inelegans theorema*": *Corr*.I,24), 还有进一步关于三角数、五角数以及立方数之和等陈述时, 说道:"对于它们的证明将使分析极大地丰富". 他发现了一个注定要缠绕其一生的课题.

哥德巴赫的另一封信很快将他送回到了费马以及沃利斯的《代数》那里. 费马说过, 一个三角数 $\frac{1}{2}n(n+1)$ 不可能是个四次幂 (*Fe*. I,341;II,406; 参看前面的第二章 §10). 哥德巴赫以为他已在 1724 年的《*Acta Eruditorum*》中证明了这样的数甚至不是一个平方数, 并在 1725 年把他的"证明"告诉了尼古拉斯和丹尼尔 · 伯努利 (*Corr*.II,170,237,239) 以及在 1730 年也告诉了欧拉 (*Corr*.I,34). 欧拉立即指出它的错误; 如果令 $x=2n+1$, 该问题等同于 $x^2-8y^2=1$ 从而这是"佩尔方程"的一个特殊情形. 他写道 (*Corr*. I,37):"这样的问题曾在沃利斯与费马之间引起过激烈的争论" (《*Commercium*》有一个清晰参考资料), "…… 而英国人佩尔对它们设计了一个在沃利斯的著作中叙述过的方法". 佩尔的名字频繁出现在沃利斯的《代数》中但从来就没有和冠以他名字的方程 $x^2-Ny^2=1$ 有过任何关联, 却由于欧拉的张冠李戴, 他的名字就被附着其上了; 由于"佩尔方程"这个习惯上的名称没有引起歧义而且方便, 尽管是个历史性的错误, 我们将继续使用它. 显然欧拉所指的方法是沃利斯归功于布龙克尔的一个方法 (*Wal*.II,797; 参看 *Wal*.II,418–429, 以及前面的第二章 §8).

欧拉在那些日子里必定是个心不在焉的读者. 即便如此, 仍有一个小小的困惑难以解释. 不仅欧拉表达了费马没有证明他的四平方和的断言的观点 ("*neque demonstrationem ejus habuisse videtur*": *Corr*.I,35;1730; 参看 *Eu*.I-2,33 于 E54 中;1736), 而且起初他似乎确信费马从来就没有说过他已证明了它 ("*neque ipse Fermatius demonstrare se posse affirmat*": *Corr*.I,30;1730). 在那时已发表费马的著述中, 只有两节包含了这个陈述. 其中一个大概是就是欧拉注意到的那个, 是在费马给迪格比的信《*Commercium Epistolicum*》中的 no. XLVII

(*Fe*.II,403= *Wal*.II,857–858 中的 no. XLVI), 这是欧拉于 1732 年连同费马 1679 年的《 *Varia Opera* 》一起作为关于 $2^{2^n}+1$ 的猜想的参考文件引用的 (*Eu*.I-2,2 于 E26 中;1723); 另一个是在费马的《丢番图》中 (*Fe*.I,305, Obs.XVIII); 在这两个场合费马都强调地宣称他拥有完整的证明. 在 1742 年, 欧拉写信给克莱罗时, 他不仅把前面的那一段话正确地复述了, 而且表达了对于费马确实有过一个证明的信任, 并对他的手稿遗失表示惋惜:"*Ce seroit un grand avantage... si l'on publioit ces démonstrations, peut être que les papiers de ce grand homme se trouvent encore quelque part*"["如果这些证明发表了的话将会是非常好的事; 也许这位伟人的手稿仍可以找到"; *Eu*.IV A-5,124]. 欧拉是什么时候改变看法的?

同样令人吃惊的是重新发现费马定理 $a^{p-1}\equiv 1 \pmod p$ 的故事, 其中 p 为素数而 a 与 p 互素. 欧拉早在 1731 年就已关注于此了. 在生命后期, 当返回到对模 p 乘群的研究期间里, 他称其为 "*theorema eximium, a Fermatio quontam prolatum*" ["费马曾给出过的最杰出的定理"; *Eu*.I-2,510 于 E262 中;1755]. 但在他早年的日子里, 我们知道他便开始从事了所设想的 $2^{2^n}+1$ 为素数的研究, 其情形与费马在几乎一百年前所做的一模一样, 而他显然完全不知道他可轻易地在费马的《 *Varia Opera* 》上 163,177 页 (*Fe*.II,209,198) 看到现成的东西. 他从观察 $2^{p-1}-1$ 是 p 的倍数开始, 这里的 p 是个素数, 在 1731 年 11 月将它寄给哥德巴赫时称其为 "*theorema non inelegans*"(*Corr*.I,60); 而后, 通过实验性 ("*tentando*": *Eu*,I-2,1 于 E26 中;1732), 他发现了 $a^{p-1}-b^{p-1}$ 当 a 和 b 与 p 互素时是 p 的倍数, 同时发现了对于费马猜测的反例 $2^{32}+1$ (参看第二章 §4). 到 1735 年 6 月, 欧拉在写信给但泽 (Dantzig)*8 的 Ehler时至少已模模糊糊地注意到了费马在 1640 年写给梅森的信 (*Fe*.II,195–199): "*Theorema...non est novum, sed ni fallor a Fermatio assertum, at sine demonstratione, ex sola inductione*"["该定理 ($2^{p-1}\equiv 1 \pmod p$) 不是新的; 如果我没搞错的话它是由费马陈述而没有给出证明的, 仅仅通过归纳得到的": *PkU*. 235]; 这可是面对了费马多次重复说他已经 (有点困难地, "*non sans peine*", *Fe*.II,198) 找到了一个证明这样的话的. 欧拉写给 Ehler 时给出了一个多少有点笨拙的证明, 它基于对 $(1+1)^{p-1}$ 的二项式公式的应用和适当重新排列各项; 在 1736 年他又再次证明了它但对其添加了基于 $(a+1)^p$ 的二项式公式的对费马定理的加法证明 (*Eu*.I-2,33–37=E54;1736; 参看第二章 §4). 然而直到 1752 年甚至更后, 他似乎都没有清楚留意到费马在这方面的优先地位 (*Eu*.II-5,141 于 E182 中). 显然欧拉在其年轻的日子里远没有集中思想去密切注意先辈们的遗赠.

---

*8波兰北部城市, 现称格但斯克; 但泽是其古称.

§3.5 角色一览表 (*Dramatis personae*)

有时一出戏剧的正戏之前有一个简短的"按出场先后"的角色介绍. 相似地, 在着手对欧拉的算术工作的详细叙述之前, 并且免不了一些重复的情况下, 我们在这里以编年史的观点, 按照它们出现在其著述和信件中的先后, 列出它的主要课题. 其中有些已被他分类到分析而不是数论中; 但是他也充分注意到了那些领域之间的联系. 正如他曾经观察到的, 当通过形式幂级数的方法证明一个算术定理时: "由此, 人们可以看出无穷小分析是如何紧密, 如何奇妙地不仅与通常的 (即代数的) 分析而且甚至与数论相关联, 但不一样的是后者似乎与更高水平的微积分相关" ["*ex hoc casu intelligere licet, quam areto et mirifico nexu Analysis infinitorum non solum cum Analysi vulgari, sed etiam cum doctrina numerorum, quae ab hoc sublimi calculi genere abhorrere videtur, sit coniuncta*", *Eu.*I-2,376 于 E243 中;1751; 参看下文的 §19].

(a) 费马定理, 模 N 的整数乘法群, 以及群论开端 (参看 §6,§7)

欧拉对数论的研究始于 1730 年的关于 $2^{2^n}+1$ 的费马猜想 (*Corr.* I,18;1730 年 1 月 8 日; 参看前面的 §4) 以及 1731 年或 1732 年的关于费马的实验性发现; 1735 年得到对它的加法式的证明 (*PkU.*295). 大约在同一时间欧拉重新发现了巴歇对于方程 $ax-by=m$ 或者等价地, 同余式 $ax\equiv m \pmod b$, 或者二重同余式 $z\equiv p \pmod a$, $z\equiv q \pmod b$ 的解 (*Eu.*I-2,18–32=E36;1735), 当然用的是欧几里得辗转相除法, 并且显然不知道巴歇、费马和沃利斯已经知道过这个结果, 更不要说Āryabhaṭa 了 (参看前面的第二章 §13, 和第一章 §4). 在我们看来, 它的主要特征是它建立了模 N 的与 N 互素的整数同余类的群的性质, 他证明了如果 a 和 b 与 N 互素, 则存在一个与 N 互素的 x 使得 $ax\equiv b \pmod N$; 不错, 这就是欧拉因此而在以后年代里所使用的一个性质 (参看, 譬如 *Eu.*I-2,350 于 E242;1751,*Eu.*I-3,8 于 E283;1760,*Eu.*I-3,521 于 E554 中;1772, 等).

对于模素数 p 或者更一般地模任意整数 N 的整数乘群 (此群现在大多数情形下写为 $\mathbb{F}_p^\times$) 的更为系统的研究, 我们需要等到欧拉在柏林的时期, 在他对二次型 mX^2+nY^2 的实验性结果中找到了对此的启示之后了. 自此以后, 欧拉的进展可以通过他的源源不断的文章流以及遗作《*Tractatus*》来追踪. 其中的这部遗作明显是在 1750 年写成的, 而后却放弃, 没有发表 (*Eu.*I-3,182–283; 参看下文的 §6). 在这里我们仅标记出这个进展过程中的一些主要阶段: 从 1747 年起, 二次剩余与 m 次剩余; 然后模素数的同余式 $x^m\equiv 1$ 的解的个数, 此处第一次 (在 1749 年) 使用了差分论证; 在《*Tractatus*》中对费马定理的乘法 (即群论的) 证明以及推广的"欧拉定理" $a^{\varphi(N)}\equiv 1 \pmod N$, 其中 a 为任意与 N 互素

的整数; 最后, 在 1772 年, 模任意素数的 $\varphi(p-1)$ 个 "原根" 的存在性及其一些主要的推论.

(b) *平方和与 "初等" 二次型* (参看 §9,§11)

我们已知 (参看 §4), 欧拉早期着迷于费马关于四平方和、三个三角数和等断言 (*Corr.*I,24; 1730 年 6 月 25 日). 最初, 正像费马那样 (参看第二章 §5), 他只是做了些很平凡的注解, 说没有形如 $4m+3$ 的, 或者更一般的形如 $n^2(4m+3)$ 的整数是两个平方数之和, 以及没有形如 $n^2(8m+7)$ 可以是三个平方数之和 (*Corr.*I,44;1730 年 10 月 17 日); 这当然利用写成模 4 或 8 的同余式容易得到证明. 1741 年, 他提到 "很长时间" 以来就已知道 $4mn-m-1$ 当 m,n 为正整数时不可能是一个平方数 (*Corr.* I,107), 但很快被证实 (*Corr.*I,114) 在此他依靠了费马的一个陈述, 即, 对于 a, b 互素, a^2+b^2 没有形如 $4n-1$ 的因子, 由此的确容易得到它. 只是到了 1742 年他才能寄给哥德巴赫一个对后一个问题的证明 (*Corr.*I,115), 当然这是基于费马定理 $a^{p-1}\equiv 1 \pmod p$ 的.

这是在证明所有费马关于两个平方数和的七年战役中第一个阶段 (参看 *Corr.*I,134;1742,313;1745, 415–419;1747; *Eu.*I-2,295–327;1749 年 3 月 20 日), 在结尾时, 欧拉成功地向哥德巴赫叙述了他的最终胜利: "现在我终于找到了一个终结性的证明······" ("*Nunmehr habe ich endlich einen bündigen Beweis gefunden...*"; *Corr.*I,493–497; 1749 年 4 月 12 日; 参看 *Eu.*I-2,328–337;1750). 在此期间及从 1747 年往后, 我们发现在欧拉的信和哥德巴赫的回信里越来越频繁地提到三个和四个平方数和, 并且, 与它们相关联的提到三个和四个变量的正交变换 (譬如参看, *Corr.*I,440;1747, 515–521;1750 以及 *Eu.*IV A-5,468,478–480;1770). 对于四平方和恒等式的决定性发现则是在 1748 年通知哥德巴赫的 (*Corr.*I,452; 参看 *Eu*,I-2,368–369 于E242 中;1751 以及 *Eu.*I-6,312 于 E407 中;1770). 在欧拉给哥德巴赫的关于两个平方数之和确定性的证明的同一封信里, 他也已能够给出一个基于他的新恒等式的证明, 证明了每个整数总是四个有理数的平方和 (*Corr.*I,495–497; 参看*Eu.*I-2,338–372=E242;1751). 至于费马原来的四平方和的断言则留给了拉格朗日在 1770 年完成最后的一步 (*Lag.*III,189–201); 但欧拉立即以一篇漂亮的论文跟了上来 (*Eu.* I-3,218–239=E445;1772), 给出了他自己对两个平方数和证明的新变形, 从而表明了它不但可应用于形式 X^2+2Y^2, X^2+3Y^2, 而且也可应用于四平方和. 至于 "初等" 二次型 X^2+AY^2, $A=\pm 2,3$, 其理论对于费马来说是已知的, 至少是它的主干部分 (参看第二章 §12), 欧拉从 1752 年起一直在研究它 (*Corr.*I, 597;1752; 参看 *Eu.*I-2,467–485 在 E256 中;1753 以及 *Corr.*I622;1755), 在 1759 年对 $A=3$ (*Eu.*I-2,556–575=E272;1759), 并直至在 1772 年对 $A=\pm 2$ (*Eu.*I-3,274–275 与 E449;1772) 最终取得了完美的结果.

(c) *二次丢番图方程*

这个话题也十分清楚地出现在欧拉与哥德巴赫的通信上 (*Corr.*I,30–31,36–37;1730; 参看前面的 §4), 在那里特别指出方程 $y^2 = ax^2 + bx + c$ 的无穷多个整数解可以由一个已知解 (不管如何得到的), 并结合 "佩尔方程" $X^2 - aY^2 = 1$ 的解推导出来. 那些结果在 E29;1733 (=*Eu.*I-2,6–17) 有所叙述并有一次以完整细节的形式出现在 E279;1758 (=*Eu.*I-2,576–611; 参看 *Corr.*I,629;1755) 以及 E323;1759(=*Eu.*I-3,73–111) 中, 其中佩尔方程 $X^2 - aY^2 = 1$ 与 $\sqrt{a}$ 的连分式之间的关系第一次被表现出来 (参看下文的 (f)).

以整数或有理数解方程 $y^2 = ax^2 + bx + c$ 重新出现在欧拉的《代数学》中, 其写作年代应不迟于 1767 年 (*Vollständige Anleitung zur Algebra*, 2 vol., St. Petersburg 1770:*Eu.*I-1,31–498=E387,388); 拉格朗日在给达朗贝尔的信中形容该书的最后一节 (Von der unbestimmten Analytic: *Eu.*I-1,326–498) 为 "论述丢番图方程的真真实实的杰出论文"("*un traité sur les questions de Diophante, qui est à la vérité excellent*": *Lag.*XIII,181;1770). 最后在 1772 年欧拉将他的结果推广到两个变量的最一般的二次方程的求整数解上 (*Eu.*I-3,297–309=E452); 令人十分好奇的是, 在论述有理解的那篇文章的前言节中, 没有提到拉格朗日关于这个论题的重要论文 (*Lag.*II,377–535;1768,655–726;1769; 参看前面第二章 §14, 以及第四章 §3), 而这是在他与欧拉在 1770 年的信件往来中的主要议题 (*Eu.*IV A-5,466–467,471–476,477; 参看以上 §2).

(d) *亏格 1 的丢番图方程, 以及其他* (参看 §14 及 §16).

这种问题, 包括传统的解法, 可追溯到丢番图 (参看第一章 §10 以及第二章 §15), 而这些对欧拉来说从学生时期就已相当熟悉了. 在 1724 年我们发现他的好朋友丹尼尔 · 伯努利在教哥德巴赫如何运用那些方法, 并且提到他自己早年就对这些东西感兴趣[1] (*Corr.*II,202–203;1724; 参看同前, 190;1723). 那时丹尼尔还不知道将传统方法加以迭代可以产生出无穷多个解 ("*quod impossibile censeo*", *Corr.*II,203); 他终于在 1730 年发现了这个办法 (*Corr.*II,356). 我们或可想象在那时他和欧拉在一起正讨论着这个问题的情景; 1730 年欧拉提到他试图将其推广到方程 $y^2 = P(x)$ 的没有结果的努力, 这里 P 的次数为 3, 而这个想法他刚刚成功地运用在 P 的次数为 2 的情形 (*Corr.*I,37).

一些年后, 欧拉用了一整篇文章 (*Eu.*I-2,38–58=R98;1738) 致力于详细处理

[1] 在 *Corr.*II,202 中的 "*sextum vel septimum*" 肯定是个错误, 或者是对 "*decimum sextum vel septimum*" 的印刷错误; 参看 *Corr.*II,190. 丹尼尔不可能在他 "6 岁或者 7 岁" 时已经解决了困难的丢番图方程.

方程 $x^4 \pm y^4 = z^2$, $x^4 \pm y^4 = 2z^2$ (参看丹尼尔给他的信,*Corr.*II,451;1738); 他查阅了弗莱尼柯的《论数的直角三角形》(参看第二章 §10), 这是被重印在巴黎科学院的《*Mémoires*》, vol.V (1729) 中的, 但或许由于刚到彼得堡的缘故, 无疑还不熟悉费马本身的证明 (*Fe.*I,340–341,Obs.XLV; 参看第二章 §10). 他还补充证明了没有一个三角数能够是个四次幂 (参看前面的 §4, 以及第二章 §10) 和对方程 $x^3 \pm 1 = y^2$ 的处理.

终于他留意到费马关于方程 $x^n + y^n = z^n$ 的断言了 (*Corr.*I,445–446;1748); 他在 1753 年 (*Corr.*I,618) 称它是 "一个非常漂亮的定理", 并补充说他可以对 $n = 3$ 和 $n = 4$ 证明它, 但其他则不行 (参看 *Corr.*I,623;1755); 对于 $n = 4$ 这事实上包含在他的 1738 年的结果中. 对于 $n = 3$ 的他的结果必定是那种结合了费马的下降法与二次型 $X^2 + 3Y^2$ 理论的证明 (参看下文的 §14); 他已经实质上利用了源自费马用来处理丢番图问题的 "初等" 二次型 $X^2 - 2Y^2$ (*Eu.*I-2,223–240=E167;1748).

在五十年代欧拉还仔细研究了丢番图, 希望能对那些偶然得到的所有看似他的著述中理出头绪来 (*Eu.*I-2,399–458=E253,255;1753–1754). 他确实成功地分离出几个希腊几何学家所钟爱的技巧, 但除此而外他的努力结果令人失望; 只是后来代数几何的发展才使得那个甚至完全模糊的课题被阐述清楚. 或许这就是为什么在欧拉逗留柏林的后期中他对此的兴趣似乎突然停止的原因吧. 他只是在写他《代数学》的最后一节时才又回到这个课题, 这一节确实像拉格朗日说的那样是个杰出的论述, 但即便有, 也没有包含多少新的东西.

自此以后, 丢番图问题似乎成了欧拉的一个主要娱兴. 值得注意的是一系列全都写于 1780 年却全都只发表于 1830 年的文章 (*Eu.*I-5,82–115,146–181=E772, 773,777,778), 它们首次考虑了丢番图方程 $\Phi(x,y) = 0$, 其中 Φ 是个对 x 为二次, 对 y 也为 2 次的多项式; 到这时在欧拉的工作中的这个课题与椭圆积分之间的关系才表现得最清楚 (参看 §15,§16).

(e) **椭圆积分** (参看 §15).

欧拉知道, 莱布尼茨和约翰 · 伯努利已经问过, 是否微分

$$\omega = \frac{dx}{\sqrt{1 - x^4}}$$

的积分可以用对数函数或三角函数来表示, 并猜测答案是否定的. 当欧拉在 1730 年问着同一个问题 (*Corr.*I,47,51), 并且而后在 1738 年给出了关于丢番图方程 $X^4 - Y^4 = Z^2$ 的费马定理的证明时, 可以确信在他头脑里必定闪现过那样的想法, 即任意将 ω 变换为有理微分的变量变换完全可以给出 $z^2 = 1 - x^4$ 的有理解, 从而给出费马方程的整数解. 在他想来, 这或许对诸如像 $\int \omega$, 以及更一般

的, 从椭圆、双曲线以及双纽线产生的积分, 增添了一些有特色的风味 (参看譬如 *Eu.*I-20,8–20=E52;1735 以及 *Eu.*I-20,21–55=E154;1749); 他也在应用数学有关的问题中, 在探讨所谓的 "弹性曲线 (elastic curve)" 中遇到过这样的积分 (参看他给约翰 · 伯努利 1738 年 12 月 20 日的信, *Bibl.Math.*(III)5 (1904),p.291, 以及他 1744 年的关于变分法论文的附录 "*De curvis elasticis*",*Eu.*1-24,231–297 于 E65 中).

然而只是到了 1751 年当法尼亚诺的《*Produzioni Matematiche*》到了在柏林的欧拉的手上时, 才使他看清了这个尚待探索的内涵丰富的研究领域. 在收到这些书的一个月后, 他就已向柏林科学院宣读了他一系列长文章 (从 *Eu.*I-20,58–79=E251 到 *Eu.*I-21,207–226=E676;1777) 中的第一篇研究报告 (*Eu.*I-20,80–107=E252;1752), 最初只是涉及法尼亚诺所考虑的那些积分, 但却一直通向了对形如

$$\int \frac{F(x)dx}{\sqrt{P(x)}}$$

的加法与乘法定理的证明, 其中的 $P(x)$ 是个四次多项式, F 为任意的多项式或者甚至是有理函数. 同时他还得到微分方程

$$\frac{dx}{\sqrt{P(x)}} = \pm\frac{dy}{\sqrt{P(y)}}$$

的具有 "典则形式" $\Phi(x,y)$ 的通积分, 这里的 Φ 分别对 x 和 y 为二次. 如在前面的 (d) 注意到的, 这后来转到丢番图方程理论了.

(f) *连分式、佩尔方程和递归序列* (参看 §12).

在欧拉给哥德巴赫的信中, 连分式的第一次出现与里卡蒂 (Riccati) 微分方程有关 (*Corr.*I,58–59;1731,63;1732), 但很快它就有了算术背景 (*Corr.*I,68;1732); 那时, 欧拉已经注意到周期的连分式,"递归序列" (即序列 (p_n) 使得对于所有的 $n \geq 2$ 有 $p_n = ap_{n-1} + bp_{n-2}$; 参看 *Corr.*I,30;1730) 与二次无理数之间的关系 (参看 *Corr.*I,36;1730). 当然, 他利用了欧几里得辗转相除法来解方程 $ax - by = \pm 1$ (*Eu.*I-2,20–21 于 E36 中;1735; 参看前面的 (a)) 也等于是构造了 a/b 的连分式 (参看 *Corr.*I,243;1743,299–301;1744), 这可能从一开始对他来说就是显而易见的, 也可能在 1737 年才彻底弄清 (*Eu.*I-14,194–196 于 E71 中), 另外又在他的 1748 年的伟大著作《无穷分析导论 (*Introductio in Analysin Infinitorum*)》中的第 18 章有清楚的阐述 (*De fractionibus continuis, Eu.* I-8,362–390).

他追踪这个主题的各个方面很多年 (作为前面提到的《无穷分析导论》第 18 章的补充, 参看 *Eu.*I-14,187–215=E71;1737, *Eu.*I-14,291–349=E123;1739, 以及 *Eu.*I-15,31–49=E281;1757); 但是连分式算法在解佩尔方程中所起的作用只是在

1759 年的一篇论文中才得到清楚阐述, 该文首先于 1767 年在彼得堡发表 (*Eu*.I-3,73–111=E323), 它很可能给了拉格朗日完全处理这个问题的最终线索 (参看第四章 §2).

(g) $\zeta(2\nu)$ 的和以及相关的级数(参看 §17,§18,§19,§20).

欧拉早年最杰出的发现之一是他对级数 $\sum_1^\infty n^{-2}$, 以及更一般的 $\sum_1^\infty n^{-2\nu}$ 的求和, 用现代的记号表示即对于所有的正偶数 2ν 的 $\zeta(2\nu)$ (*Eu*.I-14,73–86=E41; 1735); 或许这也是一个使他建立了持续高涨的声誉的一个发现吧. 这是个著名的问题, 首先由 P. Mengoli 于 1650 年正式提出 (参看 G. Eneström,*Bibl.Math*(III) 12 (1912),p.138); 它顶住了所有早期分析学家的努力, 其中包括莱布尼茨和伯努利们 (参看, 譬如莱布尼茨给约翰 · 伯努利的信, *Math. Schr.* I-3,454;1697, 以及约翰 · 伯努利给欧拉的信,*Corr*.II,15;1737). 有点独特性的是, 在解决它之前, 欧拉进行了广泛的数值计算, 以便得到对这些和数好的近似; 似乎大体上怀着这种目的, 他发展了习惯上称之为 "欧拉 – 麦克劳林求和公式" 的方法, 并依此方法重新发现了 "伯努利数", 而这个数对于数论的真正重要性要到下一个世纪才方能显现出来 (*Eu*.I-14,42–72=E25;1732,*Eu*.I-14,108–123=E47;1735; 参看 1755 年《*Institutiones Calculi Differentialis*》的第二章第五部分, *Eu*.I-10,309–336).

欧拉在 1735 年的发现是 $\zeta(2) = \pi^2/6$, 以及更一般地, 对于 $\nu \geq 1$, $\zeta(2\nu) = r_\nu \pi^{2\nu}$, 其中 r_ν 是个有理数, 最终发现它原来与伯努利数紧密相关. 最初 $\zeta(2)$ 和至少后续几个 $\zeta(2\nu)$ 的值, 欧拉是通过将牛顿关于一个有限次方程的根的幂次和的结果径直地应用到 $1 - \sin(x/a) = 0$ 这种类型的超越方程得到的. 采用这种方法对他来说如履薄冰, 当然, 他知道这一点.

彼得堡的出版是缓慢的; 但很快欧拉将消息传送给了全欧洲的朋友和同事们, 从而它成了在他与他的一些通信者之间活跃的讨论话题. 与此同时他仍不遗余力地强化他的方法. 在他的首次发现之后不到十年的时间里, 他已能够在他的《无穷分析导论》(于 1748 年在瑞士洛桑出版, 但在 1744 年已成文; 参看 *Corr*.I,292;1744) 里包含了关于它的完整的阐述, 按他的标准这是一个完全满意的结果, 甚至按我们更高的要求看在实质上也是如此. 它基于对三角函数及其展成的无穷级数和无穷乘积的细致处理 (*Eu*.I-8,133–212=《无穷分析导论》的第 8–11 章), 为此他加上了关于 $\zeta(s)$ 的 "欧拉积" 和各种 L- 函数的整整一章 (同上, 284–312= 第 15 章). 至于他为获得奇整数 $n > 1$ 时 $\zeta(n)$ 的信息的努力, 无疑是没有成功的, 因为直到现在对此问题也几乎没有取得什么进展. 但是这些努力也并非完全没有成果; 事实上在寻求这种信息时欧拉偶然发现了 $\zeta(s)$ 的函数方程及其相伴的级数

$$L(s) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}$$

(*Eu*.I-15,70–90=E352;1749). 这仅仅作为一些令人好奇而并不真正了解的东西留了下来, 直到 1859 年它们在黎曼的手中才获得了新的生命.

(h) “数的分拆 (*Partitio numerorum*)” 和形式幂级数(参看 §21)

1740 年一个法国裔柏林数学家 Ph. Naudé 写信给欧拉, 问道 (其中的一个问题), 一个给定的整数 m 可以有多少种方式分成 μ 个不同的整数和. 欧拉几乎是立刻就回答了他 (*PkU*.193) 并在几个月里把此问题深入下去, 向彼得堡科学院提交了一份学术论文, 这时正好在他离开彼得堡前不久 (*Eu*.I-2,163–193=E158;1741 年 4 月 6 日). 他在许多场合都回到了这个课题, 并在他 1748 年的《无穷分析导论》的一章中 (第 14 章 =*Eu*.I-8,313–338) 以及在 1768 年最后一次 (*Eu*.I-3,131–147=E394) 较详细地论述了它.

他立刻看出 Naudé的问题的关键在于考虑一个适当的诸如 $\prod_{i=1}^{\infty}(1+x^iz)$ 和 $\prod_{i=1}^{\infty}(1-x^iz)^{-1}$ 的形式幂级数. 在处理它们时他立即遇到了令人瞩目的无穷乘积

$$\prod_{i=1}^{\infty}(1-x^i)=1-x-x^2+x^5+x^7-\cdots+x^{51}+\cdots$$

(*Eu*.I-2,191 于 E158 中;1741), 在将它展成如上所示的幂级数时, 它必定使他感到震动; 不仅所有的非零系数均为 ±1, 而且很容易认出这些幂指数均为 “五角数” $\frac{1}{2}n(3n+1)$. 这差不多花了十年时间才使他能够向哥德巴赫送去对此的一个证明 (*Corr*.I,522–524;1750).

就像雅可比认识到的那样, 这类事物的完全解释必须要到 θ- 函数和模形式的理论中方能找到. 这远远超出了欧拉的视野. 当他告诉哥德巴赫说, 证明费马关于四平方和的定理应该考虑级数 $\sum_{n=1}^{\infty}x^{n^2}$ 四次幂 (不完全是 θ- 级数 $\sum_{n=-\infty}^{+\infty}x^{n^2}$, 但接近它) 时, 我们不得不羡慕他的预言的威力. 这也不得不等着雅可比的到来.

(i) 二次型的素因子(参看 §8,§9)

§3 中所引的给哥德巴赫的同一封信是在欧拉到达柏林时几乎立刻写就的 (*Corr*.I,105–107;1741 年 9 月 9 日); 在这封信里包含了一些有纪念意义的数学资料: 首先, 如在前面的 (b) 中提及的, 关于 $4mn-m-1$ 的, 即本质上是关于二次型 X^2+Y^2 的因子的结果; 然后是许多由 “归纳法” (即实验) 得到的陈述, 这是些有关二次型 X^2-2Y^2, X^2-3Y^2, X^2-5Y^2 的素因子的; 最后还有他的关于积分

$$\int_0^1\frac{dx}{(1-x^n)^{p/q}}$$

的第一个结果 (后来它以 "第一类欧拉积分" 为人所知).

当欧拉在几个月后写信给克莱罗, 回应他的关于在柏林职业方面的询问时说, 他在那里 "享受完全的休息" ["*je jouis...d'un parfait repos*":*Eu.*IV A-5,110;1742 年 1—2 月] 同时在等待国王对他的学术活动的关注; 显然他把他的休闲时段转换成了一个紧张的创造时段了, 特别是在数论领域中的创造活动. 在一年内, 他已经将他的注意力拓展到一大类的二次型 $X^2 + AY^2$, 其中 A 为正或负的整数 (*Corr.*I,146–150;1742 年 8 月 28 日, 161–162; 1742 年 10 月 27 日; 参看同上索引, 260;1743 年 10 月 15 日). 在 1742 年 8 月他已经十分接近于二次互反律了, 并且强调了他的发现的价值, 他写道:" 我确实感觉到我离穷竭这个课题相隔甚远; 然而数的那些非数值的许多光彩夺目的性质仍然待以发现" ["*Ich glaube aber fest, dass ich diese Materie bei weitem noch nicht erschöpfet habe, sondern, das sich darin noch unzählig viele herrliche proprietates numerorum entdecken lassen...*", *Corr.* I,150]. 他恰如其分地将这样的重要性附加在他为之不倦重复的猜想上直至生命的终结, 尽管朝着这个猜想的证明方向没有什么进展, 但它或多或少地具有了准确的形式 (可参看 *Eu.*I-3,280–281 于 E449;1772, 以及 *Eu.*I-4,163–196=E598;1775, 后面的这篇论文基于拉格朗日 1775 年的《*Recherches d'Arithmétique*》). 二次互反律的清晰陈述出现在 1772 年的一篇文章的最后结论中 (*Eu.*I-3,512 于 E552 中;1772), 发表于 1783 年欧拉的《*Opuscula Analytica*》中, 这正是他逝世的那一年.

(j) 大素数 (参看 §10).

当从事于费马数 $2^{2^n}+1$ 研究的 1730 年时, 欧拉已经遇到了决定一个给定的大整数是否是素数的问题. 费马已经知道了(参看第二章 §9) 一个形如 $4n+1$ 的非平方整数为素数当且仅当它有且只有一个两个平方数之和的表示, 而此表示中的两个平方数是互素的. 第一次提到欧拉对这个判别法的再发现出现在 1742 年 (*Corr.*I,134–135). 在 1749 年刚刚在完成关于两平方数之和的证明 (参看前面的 (b)), 欧拉便将这个判别法应用到了各种素数及非素数 (*Eu.*I-2,321–327 于 E228 中). 他在 E283;1760(*Eu.*I-3,1–45) 和在 E369;1765(=*Eu.*I-3,112–130) 中更加系统地描述了这个一样的方法; 在较前的一篇文章里, 欧拉更为特殊地研究了形如 a^2+1 的素数并且也给出了解模给定素数 $p = 4n+1$ 的同余式 $x^2 \equiv -1$ 的方法 (基于欧几里得辗转相除法, 参看前面的 (a) 和 (b)).

最后, 在他老年时, 欧拉把费马的判别法推广到了具二次型 $mX^2 + nY^2$ 的大数, 并将这个结果知会了他的朋友, 前柏林的同事, 瑞士数学家 Béguelin (*Eu.*I-3,418–428=E498 以及 708_a;1778; 参看 *Eu.*I-4,269–289,303–328,352–398=E708, 715,718,719,725;1778). 这基于了 "*numerus idoneus*" 即 "合适的数" 的概念. 根

据原创的、多少有点不严格制定的定义, 称一个数 N 为 "合适的" 是说, 当 (且仅当) 每个可以写为且以唯一方式写为 a^2+Nb^2 的奇整数是个素数, 其中的 a 与 b 互素; 并断言所有使得 $mn=N$ 的形式 mX^2+nY^2 于是也有同样的性质. 最终在摒弃了一些特殊设定的平凡情形后, 它被进行了修订. 欧拉至少也找到了一个具启发性的方法, 用以决定一个数 N 是否在他的意义下是 "合适的" (即对用推广了的费马判别法测试大数的素性是合适的); 他列出了从 1 到 1848 中 65 个这样的数, 并用它们发现了一些大素数 (大于 10^7), 这是些过去不知道的数.

在高斯的《算术研究 (*Disquisitiones Arithmeticae*)》中, 他指出欧拉的 *numeri idonei*, 准确地说, 是那些对每个种数有且只有一个类的二次型的行列式, 从而在一定程度上澄清该问题. 当欧拉进行研究哪些整数可以写成 mx^2+ny^2, 其中 x, y 为有理数, 而 m, n 为已知整数时, 他已经遇到了隶属于种的理论的问题 (*Eu*,I-4,I-24=E556;1772; 参看 *Corr*.I,605;1753).

§3.6 模 N 的乘法群

我们以费马定理为起点 (参看前面 §4, 以及第二章 §4). 费马在试图分解诸如 $2^n\pm1$, $3^n\pm1$ 等的数时发现了它. 我们已经看到, 可以或者用加法方式进行阐述和证明, 而证明的方法基于了二项式定理, 或者按乘法的方式进行. 费马对它的最后一次阐述 (*Fe*.II,209) 是按后一种方式的, 由此可以推测他已证明了它, 尽管他自己发现的关于二次项系数的信息 (参看第二章 §2) 已足以能给出其他的证明了.

欧拉对这个问题的兴趣产生于哥德巴赫对费马关于数 $2^{2^n}+1$ 的猜想的执着 (参看前面的 §4). 不知不觉地踩着费马的脚印, 他开始以实验来发现定理, 起初是 $2^{p-1}-1$ 的情形, 然后再是一般的 (参看 §4). 但对照于费马, 他几乎将二项式定理当作源泉来吸收; 因此对于他的第一个证明是加法方式的并不令人感到奇怪 (*Eu*.I-2,33–37=E54;1736; 参看 *PkU*.295;1735).

在柏林当他以适当的热情从事两个平方数之和的研究 (参看下文的 §9) 时, 费马定理曾成为他的第一个结果的主要成分 (*Corr*.I,115–116;1742; 参看第二章 §7, 以及下文的 §9); 但这还没有给他提供一个动机, 以寻找一个用模素数的整数的乘法性质来证明费马定理. 人们试图在 "*herrliche proprietates* (奇妙的性质)" 中寻求这样的一个动机, 这里的这个奇妙性质是指在 1742 年同年他按经验所发现的, 他甚至以超出惯常的很大热情向哥德巴赫叙述了它 (*Corr*.I,146–150;1742 年 8 月 28 日); 在研究了二次型 X^2+NY^2 并且对于 N 的多个值考察了该形式的素因子在模 $4N$ 下的分布 (以现代说法, 即在域 $\mathbb{Q}(\sqrt{-N})$ 中有理素数的分

解), 这是他所发现的 (*Corr.*I,148): "如果一个形如 $4Nn+s$ 的素数是 X^2+NY^2 的一个因子, 则所有形如 $4Nn+s^k$ 也如此; 如果两个素数 $4Nn+s$, $4Nn+t$ 如此, 则每个形如 $4Nn+s^kt^i$ 也如此." 事实上 (参看下文的 §8), 他不仅发现了从实质上说的二次互反律, 而且同时还有模 $4N$ 的乘群的子群概念, 更准确地说, 是那个群的指数为 2 的子群.

不管这些观察是否给了欧拉对于进一步探索群论概念的主要动机, 从 1745 年到生命的尽头他显然赋予了它们许多的思想. 与此同时他开始留意到了他的定理的费马的原创者身份 (参看前面的 §4); 或许他对于费马的清晰的乘法表述也有深刻的印象吧. 然而也可能是看到他越来越朝向对数论的概念化方式的进步令人着迷的缘故; 数论, 这是个 (这与传说他是个经验主义者没有什么抽象思维不符) 随着时光流逝而变得越来越 "现代" 的一个词汇, 它见证了这个进步.

尽管仍旧坚持对费马定理使用加法式的证明 (*Eu.*I-2,65–67 于 E134 中), 欧拉却在 1747 年认为值得指出, 就有关于以 p 相除的可除性 (其中的 p 不必为素数) 而言, 整数 a, b 等可以用 $a\pm\alpha p$, $b\pm\beta p$ 等予以置换, 就是说, 用任意使得在除以 p 时保有同样余数的整数置换 (同上, p.77, *Scholion*); 他讨论了 "由对平方数的除法产生的剩余"(或者由立方数等产生的) 并开始考虑那些由费马定理所产生的这种剩余的性质. 特别他发现 (同上 p.81, 定理 13) "如果 $a-f^n$ 可被 $p=mn+1$ 除尽, 则 a^m-1 也如此" (费马定理的一个简单的推论), 并立刻提出了证明其逆的问题, 他发现它总是对的 (同上,p.82, *Scholion*). 此后不久, 在他的第一篇关于两个平方数之和的主要论文 (*Eu.*I-2,295–327=E228;1749) 中, 我们发现了对于二次剩余的一个更加仔细的讨论, 但依然在冠以多少有点烦心的名称 "由平方数除以素数 p 产生的剩余" 之下 (同上,pp.312–313,*Scholion*); 注意, 这样的剩余的个数正好是 $\frac{1}{2}(p-1)$, 并有猜想说, 对于 $p=4n+1$, 它们恰恰是 $x^{2n}\equiv 1 \pmod p$ 的解, 它是上面所叙述的猜想的特殊情形 (将 m, n 换为 $2n$, 2); 对于两个平方数之和的问题这是个具决定性的情形.

在 1749 年他仍旧取得了进展 (*Corr.*I,493–495; 参看 *Eu.*I-2,328–337=E241; 1750), 即对同余式 $x^{2n}\equiv 1 \pmod p$ 应用差分算子从而证明了它不可能对所有与素数 $p=4n+1$ 互素的 x 都成立. 欧拉在几年之后推广了它 (*Eu.*I-2,516 于 E262 中;1755), 其论证如下. 记 D 为差分算子

$$(Df)(x)=f(x+1)-f(x).$$

由对 m 归纳知, 对于任意的 $m\geq 1$ 有

$$(D^mf)(x)=f(x+m)-\binom{m}{1}f(x+m-1)+\binom{m}{2}f(x+m-2)-\cdots\pm f(x).$$

因此, 如果对 $x=1,2,\cdots,m+1$, 素数 p 除尽 $f(x)$, 则它必定除尽 $(D^mf)(1)$. 再

由对 m 的归纳, 我们发现, 如果 $f(x) = x^\mu$, 则 $D^m f$ 当 $\mu = m$ 时为 $m!$, 而当 $\mu < m$ 时为 0; 这表明对所有的首项系数为 1 的多项式

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m$$

总有 $D^m f = m!$. 因此, 如果 $m < p - 1$, 则 $x = 1, 2, \cdots, m + 1$ 不可能满足同余式 $f(x) \equiv 0 \pmod p$, 更不要说对所有与 p 互素的 x 了.

不久我们将看到, 这个精致的论证以后被一个更强并更具结构性的论证所替代. 当它首先以以上形式出现时, 它被用于处理 1747 年留下的未解决的问题, 即证明, 如果 $p = mn + 1$ 是个素数且 $a^m - 1$ 被 p 除尽, 则 a 是模 p 的 n- 次幂剩余 (同上, pp. 515–516, 定理 19). 事实上, 假定 $a^m \equiv 1 \pmod p$, 并写出恒等式

$$x^{mn} - a^m = (x^n - a)(x^{(m-1)n} + a x^{(m-2)n} + \cdots + a^{m-1}).$$

于是费马定理表明该式的左端对所有互素于 p 的 x 是 p 的倍数, 而欧拉的推理表明右端的第二个因子不可能具有这个性质; 因此必定对某个 x 有 $x^n \equiv a \pmod p$. 令 $a = -1$ 及 $n = 2$, 该证明化成了在前面第二章 §7 证明的一个复制品, 这是欧拉曾在 1749 年送交给哥德巴赫的 (*Corr.*I,494–495; 参看前面的 §5 (b), 以及下文的 §9); 这曾是在他更早时期努力证明关于两个平方数之和的费马定理中所缺少的一个环节.

无疑受到这个成功的极大鼓舞, 而且也看到了他的《无穷分析导论》于 1748 年的付印, 于是欧拉[2]着手写一本专著, 或许想要将其作为类似于对数论的一个 "导引", 在放弃这个努力前他为此写了十六章, 它们在 1849 年出版, 书名为《*Tractatus de numerorum doctrina*》(*Eu.*I-5,182–283=E792); 在某种程度上说, 它看起来像是高斯《*Disquisitiones*》的第 I,II 和第 III 节的初稿. 它以对一些初等事项的明晰阐述开始, 主要是 (第 2–4 章) 现在通常记为 $\sigma_0(n)$, $\sigma_1(n)$, $\varphi(n)$ 的函数计算, 这些函数分别代表了 n 的因子个数, 它们的和 (欧拉的记号是 $\int n$), 以及与 n 互素且小于 n 的整数个数 (即 "欧拉函数", 欧拉后来对它使用了记号 πn; 譬如参看 *Eu.*I-4,105–115=E564;1775). 然后他进行 (第 5 章, no.140–166) 了对自高斯以后称之为相对于一个模的同余式的初等讨论; 对于模的欧拉系统用语的意思是 " 除数"[*9]. 对于一个除数 d, 称所有整数 $r + dx$ 属于同一个类

[2]不早于 1749 年, 这是因为使用发现于该年的差分算子显著地刻画出这点 (*Eu.*I-5,222,no. 256–259). 应该注意附加在该文初稿的边白的一些注解, 它们作为附言 插入到 *Eu.*I-5 中; 推测起来, 这些附言应是事后补记的; 譬如对于 no.565, p.278 的附言, 它摒弃了正文中的一个错误证明.

[*9]这里的英文仍用的 "the divisor", 和前面的 "因子" 用的同一个字 "divisor", 但意思完全不同, 甚至代数几何的除子也是 "divisor", 我们只能尽量区分了.

(no.14) 并把它们看成是“等价的” (no.154). 整数 a 的类的任一代表被称做 a 的“一个剩余”, 这个词有时 (并非总是) 限定为 a 除以 d 的一个剩余 r 使得 $a = r + dx$, $0 \le r < d$. 它也可以阐述为由整数到它们的“剩余” (在那些剩余的等价类的意义下) 的一个映射具有我们现在称作的环同态的那些特征性质.

下一章 (第 6 章) 处理了按以下方式产生的剩余: 对于给定“除数” d, 由算术级数 a, $a+b$, $a+2b$ 等的整数除以 d 的剩余, 或者用现代语言说, 是由 b 在模 d 加群中生成的子群的陪集; 当然这也等于是决定 b 和 d 的 g.c.d., 也等价于同余式 $bx \equiv m \pmod{d}$ 的解, 这个是欧拉最早期的一篇文章的主题[3] (*Eu*.I-2,18–32=E36;1735; 参看前面的 §5(a)). 这个主题在模 d 的乘群的研究中也随着被做了 (第 7 章); 它表明, 如果 b 与 d 互素, 则由 1, b, b^2 等构成一个在模 d 的乘法和除法下封闭的子集, 实际就是一个群; 由此, 当考虑与 d 互素的整数的模 d 乘群中它们的陪集集合, 便表明它的阶, 即使得 d 除尽 $b^\nu - 1$ 的最小的 $\nu > 0$, 必定除尽后面这个群的阶 $\mu = \varphi(d)$. 因此 d 必除尽 $b^\mu - 1$.

这便是欧拉的著名定理; 当 d 是个素数时, 它就化成了费马定理 (参看第二章 §4). 在以后的年代发表他的证明时 (*Eu*.I-2,493–518=E262;1775: 素“除数”情形; *Eu*.I-2,531–555=E271;1758: 一般情形), 欧拉不仅坚持认为这是一个实质性的推广, 表明了引进“欧拉函数” $\varphi(n)$ 的正确性, “否则将会是毫无结果可言” (*Eu*.I-2,555, *Scholion*), 而且还指出, 即便 d 为素数, 上述的证明也优于“加法式”的, 他说, 它是“更自然的”, 这是因为后者依赖于二项式公式, 而它似乎与主题隔得很远 (“*a proposito non mediocriter abhorrere videtur*”: *Eu*.I-2,510, *Scholion*). 他也偶然注意到, $\varphi(N)$ 一般来说对于所有与 N 互素的 x, 它并不是使得 N 除尽 $x^n - 1$ 的最小 n; 例如, 如果 $N = p^\alpha q^\beta r^\gamma$, 其中 p, q, r 为不同素数, 那么这个性质并不属于 $\varphi(N)$, 即 $p^{\alpha-1}(p-1)$, $q^{\beta-1}(q-1)$, $r^{\gamma-1}(r-1)$ 的积, 而是属于它们的最小公倍数 (l.c.m) (*Eu*.I-2,532,Summarium); 他已经在他的那个第一篇关于数论的文章里做了相似的考察 (*Eu*.I-2, 于 E26 中;1732) 但没有能证明它.

当然在模, 或以欧拉的用语, 除数是个奇素数 p 时, 最令人感到兴趣, 而我们很快就发现他在《*Tractatus*》中集中注意了这种情形 (第 8 章). 他一开始便证明了, 如果 a 与 p 互素且 p 除尽 $a^n - 1$, 则由于 p 也除尽 $a^{p-1} - 1$, 那么它便除尽了 $a^d - 1$, 其中 d 是 n 和 $p-1$ 的 g.c.d.; 实际上, 他在这里所用到的事实现在可以表达为, 模 p 的 a 的幂的剩余类群是模 $p-1$ 加群的一个同态像. 由此他推导出, 如果 n 自己是个奇素数且 p 除尽 $a^n - 1$ 但不除尽 $a - 1$, 则 p 必具有形式 $2nx + 1$; $a = 2$ 的情形适合于对完全数的研究.

[3] 十分古怪的是, 在第 1 章到第 8 章的正文中对于整数分解素因子的唯一性的正当性没有给出解释. 仅仅在那里将欧几里得辗转相除法作为一个事后补充, 在 no.139 和 no.150 的附言里提到.

不管是不是意识到 (参看第二章 §4), 欧拉依旧跟着费马走, 注意到了下一个问题 (no. 255), 即对于 $p = 2m+1$ 及互素于 p 的 a, p 除尽

$$a^{2m} - 1 = (a^m - 1)(a^m + 1),$$

从而或除尽 $a^m - 1$ 或 $a^m + 1$, 但不会同时除尽两个; 他问道是否它可以对所有互素于 p 的 a 都除尽 $a^m - 1$. 在此时刻, 他引进了他新发现的有限差分方法, 证明了这种情形是不可能出现的; 更一般地, 他利用它证明了, 如果 $n < p-1$, 则 p 不可能对所有互素于 p 的 a 都除尽 $a^n - 1$.

在这里他险些错过了证明模任意素数的 "原根" 的存在性以及所有那些他后来由此推导出的结果的机会; 这里的原根是指模 p 乘群的一个生成元. 的确, 已经掌控了这些手段的他, 便能够轻松地证明了, 如果 a 和 b 为那个群的元素 (或者一般的, 任意有限交换群的元素), 则总有一个元 $a^\mu b^\nu$, 其阶为 a 和 b 阶的 l.c.m. 因此, 如果 n 是那个群元素阶中的最大数, 它必定也是它的所有元素的阶的倍数, 故而对所有与 p 互素的 a, p 必定除尽 $a^n - 1$, 因而 n 不能 $< p-1$.

正由于部分地缺少了这个结果, 《*Tractatus*》的剩余的大部分内容是实验性的, 模糊的, 甚至完全错误的. 如果用现在称作的群论术语, 他的目的无疑是要首先给出关于二次剩余的说明, 然后是关于模 p 的 m 次幂剩余的, 至少是对 $m = 3, 4, 5$ 的. 欧拉看出, 对于每个 m, 这样的剩余构成了一个对乘法和除法的封闭集合, 他称其为: "一个真正突出的性质" ("*insignem proprietatem*": no.295), 就我们所知, 他已经在与二次型有关的地方见过它的类比物(参看下文的 §8). 用我们的话, 这是说 m 次剩余构成模 p 乘群 G 的一个子群 G_m; 欧拉甚至利用 G_m 在 G 中的陪集讨论了现在称之为的商群 G/G_m, 然而, 除了当 G_m 在 G 中指数为 2 时的 $m = 2$ 外, 他不能确定它的结构, 甚至它的阶; 他的意图是要证明对于 $m = 3, 4, 5$, 当 m 除尽 $p-1$ 时 G/G_m 为 m 阶循环群, 但这一点在那时甚至都还没有明确的意义. 很清楚, 他的计划由于过于超前而不得不放弃.

但是, 就像通常在欧拉身上所发生的那样, 什么都不会丢掉; 在《*Tractatus*》中最有价值的无论什么肯定要出现在下一个十年的出版物上. 他的 1751 年论四平方和的文章中较大部分 (*Eu.*I-2,338–372=E242, pp.339–365) 都致力于对二次剩余和非剩余的仔细阐述, 最初没有假定 "除数" (即模) 是素数. 当它是一个奇素数 p 时, 欧拉证明了这些剩余构成了模 p 乘群的一个指数为 2 的子群, 这就是所有这一切所蕴涵的, 而对于我们来说, 这似乎简直像平凡那样的初等, 但在他所处的年代这是新的, 需要仔细讲解方能明白. 特别地, 他现在可以指出, 如果 -1 是一个模 $p = 2n+1$ 二次剩余, 则二次剩余必在 $\{r, -r\}$ 这一对数中, 故而 n 必为偶数; 至于其逆他只注意到他为寻找一个 "直接" 证明 (即显然是指不依靠差分算子: p.365,*Scholion*) 的努力已无果而终.

在那篇文章里, 看起来, 其目的是要处理四平方和 (参看下文的 §9). 于是, 不过几年,《*Tractatus*》似乎已被搁置一旁; 基于它的下一篇文章令人瞩目地冠以 *Theoremata circa residua ex divisione postestatum relicta* (即, 关于模素数的 m 次剩余: *Eu.*I-2,493–518=E262) 的题目, 并在 1755 年他向柏林科学院进行了宣读; 欧拉叙述了他的有限差分法的最新版本 (前面所复制的那个), 同时还有他的对 $a^n \equiv 1 \pmod p$ 的判别法, 以判别一个整数 a 是个模素数 $p = mn+1$ 的 m 次剩余. 依次下来的是标题为 *Theoremata arithmetica nova methodo demonstrata* (*Eu.*I-2,531–555=E271;1758), 这一回它基于了《*Tractatus*》的第 4 章到第 7 章; 这里的 "新方法" 是模任意整数 N 的加群和乘群的群论式的研究, 包括对乘群的 $\varphi(N)$ 的阶的计算, 所有这一切导出了欧拉定理: 对所有互素于 N 的 a, N 除尽 $a^{\varphi(N)} - 1$.

或许除了与二次互反律有关的一些猜想和几个对于三次和双二次剩余的大胆归纳结果外, 从《*Tractatus*》也只能提取出一个超出欧拉在那个时段的能力的证明. 在一段时间里他对这种事情的兴趣减缓了; 要使它复兴需要某种外来的冲击. 拉格朗日是提供这种冲击的人.

哥德巴赫多年来一直单独地对欧拉的算术工作持有兴趣 (虽然是业余的却是真正的). 他们在 1756 年到 1762 年之间的通信几乎完全被七年战争*[10] 打断; 其间, 哥德巴赫慢慢老了; 他于 1764 年与世长辞. 拉格朗日与欧拉的通信始于 1754 年 (参看第四章 §1), 那时他只有十八岁; 他的第一封信似乎泄露出他是个生涩的初学者, 很难引起欧拉的关注; 虽然欧拉没有回信, 但颇有特点地, 他保存了它. 拉格朗日的第二封信却写于一年之后, 概述了一个完全新的和原创的对变分问题的处理, 给予欧拉一个深刻而持久的印象, 从此之后, 不管年龄的差距, 他与拉格朗日平等相待. 拉格朗日于 1736 年生在都灵, 除了在 1763—1764 年到巴黎的旅行外他生活在那里; 直到 1766 年, 那时他迁移到了柏林去接替欧拉的位置. 1787 年他最后安居在了巴黎; 那时他对数论再也没有积极的兴趣了. 他死于 1813 年.

拉格朗日许多工作如果不是说全部的话, 都是建立在欧拉工作的基础上的; 这个评价特别可应用到数论上, 对此他曾写信给欧拉说:

"*Je suis très charmé que mes recherches sur les problemes indeterminés aient pu meriter votre attention; le suffrage d'un savant de votre rang est extrêmement flatteur pour moi, surtout dans une matiere , dont vous êtes le seul juge compétent que je connoisse. Il me semble qu'il n'y a encore que Fermat et vous qui se soient occupés avec succés de ces sortes de recherches, et si j'ai été assés heureux pour ajouter quelque chose à vos decouvertes je ne le dois qu'â l'étude que j'ai faite*

*[10]指 1756 年到 1763 年的法、俄、奥与英、普 (鲁士) 之间的战争.

de vos excellens ouvrages." ["我最高兴的是我对不定方程问题的工作得到您的关注; 像您这样级别的科学家的宝贵意见对我来说是最喜欢的, 特别, 就我所知, 是在这样一个领域, 在那里您是一个也是仅有的一个有资格的评判者. 对我来说似乎只有费马和您是迄今处理这类问题的成功者, 而且, 如果我能够有幸在您的发现上添加上什么的话, 我只能将其归功于我曾学习了您的杰出工作":*Eu.*IV A-5,471;1770 年 2 月 12 日].

这不仅仅只是礼貌和恭维; 在他与达朗贝尔和其他人的通信中, 拉格朗日自己的表达更加自在, 更具批评性, 但无疑, 总是带有深深感恩和羡慕的相同情感.

这一段以及前面 §2 的那一段引语是在涉及后者的关于不定方程的文章而在欧拉与拉格朗日之间的交换信件的一部分 (*Lag.*II,377–535), 它发表在 1769 年柏林的《*Nouveaux Mémoires*》中; 欧拉在 1769 年或 1770 年初得到它们. 无疑, 部分地因为这次交换信件, 拉格朗日在 1770 年写了那篇论文的续篇 (*Lag.*II,655–726), 欧拉于 1770 年或 1771 年初收到了它 (*Eu.*IV A-5,488;1771 年 5 月 20 日); 它包含了一个证明, 证明了一个模素数 p 的 n 次同余式最多只有 n 个模 p 根 (索引同上, pp.667–669).

这正好是在欧拉写《*Tractatus*》时所遗漏的地方; 人们或可推测他很快意识到此, 并因此而修正了他关于模素数乘群的思想. 无论如何, 几乎没有超过一年时间, 我们发现他在 1772 年 5 月 18 日提交给彼得堡科学院三篇关于 m 次剩余的文章[4](*Eu.*I-3,240-281=E449,497–512 =E552,513–543=E554).

十分奇怪地, 拉格朗日的证明 (他只是顺带地对三次同余式做了明晰的处理, 但按照一般情形做了正确的陈述) 建立在了一个修订的关于有限差分的欧拉论证的基础上. 它很可能是拉格朗日事后才想到要放进他的文章中的; 无论怎样看, 在那里它都没有什么用处, 这或许也是为什么欧拉没有引述拉格朗日与此相关的东西. 欧拉对此的证明是现代的. 当今人们表达它只简明地说道, 模一个素数的整数构成一个域 (欧拉在实质上而不是在语句上对此已有充分了解), 而笛卡儿也已知道了对它的经典论证 (索引同上, 第二章 §7), 他证明了一个 n 次方程 $f(x)=0$ 最多只有 n 个根在任意域上仍然有效; 事实上, 如果 a 是一个根, 则可用 $x-a$ 去除 $f(x)$ 从而写成

$$f(x)=(x-a)f_1(x);$$

除非 $x=a$ 或者 $f_1(x)=0$, 否则它不会为 0; 由于 f_1 的次数为 $n-1$, 对 n 的归纳便证明了此断言. 为了表达这同一个思想, 欧拉注意到 (*Eu.*I-3,249), 如果 a

[4]只有第一篇出现在该科学院 1774 年的《*Novi Commentarii*》上. 其他两篇被欧拉放在了他 1783 年的《*Opuscula Analytica*》中; 或许他一直期待它们, 希望能对这类事物说得更多, 然而感到了时不我待, 他想要迅速地看到它们付印.

是同余式 $f(x) \equiv 0 \pmod p$ 的一个解, 则可记 $f(a) = mp$, 其中 m 是个整数, 故 a 是 $f(x) - mp$ 在通常意义下的一个根. 现在记

$$f(x) - mp = (x - a)f_1(x)$$

并如上面那样应用归纳法, 或者选择另外的方法 (如欧拉所做), 逐次进行相除直到所有的根已穷竭, 这便得到所要的结果.

这个定理 (顺便说一下, 仅仅在 $f(x) = x^n - 1$ 的情形做了证明, 但是此证明却是普遍有效的) 于是被用来证明模任意素数 p 的原根的存在性; 虽说有一些笨拙之处 (不管是出自欧拉还是他的助手) 使得一些细节模糊不清, 但这个证明的总体设计是清楚的. 一方面欧拉在实质上证明了对每个 n 有一个次数为 $\varphi(n)$ 的多项式 F_n (后来被称为这个次数的 "分圆多项式") 使得 $x^n - 1$ 是多项式 $F_d(x)$ 的乘积, 其中的 d 取遍 n 的所有因子 (包括 1 和 n); F_n 的根, 不管是 "实" 的还是 "虚" 的, 正好都是 n 次单位原根. 证明是用对 n 的素因子的个数的归纳进行的, 这里的根可以相同, 尽管如此, 证明也只在三个因子的情形进行 (这给了高斯一个机会, 使他能趁一时之鲁莽宣称欧拉的这个结果是 "仅仅用归纳" 证明的, 按他用语的含义, 指的是靠实验的方法); 实际上, 欧拉是用所有属于与 n 不同的 n 的因子的 "分圆多项式" 去除 $x^n - 1$ 得到 $F_n(x)$ 的. 因此, 对于每个 n, 我们可以写成

$$x^n - 1 = F_n(x)G_n(x),$$

其中 G_n 是多项式 F_d 的乘积, 而 d 是 n 的因子且 $< n$. 对于欧拉论证的有效性还需要这样的事实, 即 F_n 和 G_n 的系数应为整数; 因为它们是通过逐次除以具整系数的首 1 多项式 (即最高次项的系数为 1 的多项式) 得到的, 所以很容易看出这个事实, 不过欧拉并没有提到这一点. 于是最后一步便是取 $n = p - 1$ 并注意到多项式 $x^{p-1} - 1$ 在取模 p 后, 具有 $p - 1$ 个不同的 "实" 根 $1, 2, \cdots, p - 1$, 故而它的因子 $F_{p-1}(x)$ 必定自己就有像其次数 $\varphi(p - 1)$ 所表示的一样多的模 p 根, 而这些根是在 $1, 2, \cdots, p - 1$ 之中; 这些是模 p "原根". 此论证等于是说, 在模 p 整数域上 (或者真正地, 在任意域上), 分解成线性因式乘积的多项式的每一个因子必定自己也分解为这些因式; 尽管欧拉没有把这一点弄得十分清楚, 翻译成欧拉的语言, 还是容易看出它是成立的.

至于说到欧拉从原根存在性推出的各种结果, 在这同一篇论文中和在同一天提交给科学院的两篇相随的论文中, 一些结果对于我们来说似乎是显然的而且对于欧拉而言也的确没有耗费他什么精力; 其他一些则涉及与二次互反律有关的定理和猜想, 我们将在以后讨论它们. 值得注意的是欧拉越来越意识到, 在这些事物中, 他所处理的不是一些个体的整数而是那些我们称之为同余类的东

西, 用现代记号表示, 即处理了素域 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; 对此概念他引进了 *ordo* 这个字 (*Eu.*I-3,242), 而后则用了 *species* (*Eu.*I-3,519); 对于各自由 $\frac{1}{2}(p-1)$ 个 "*species*" 组成的模 p 二次剩余群和非剩余的集合, 它使用了词 *classis* (*residuorum, non-residuorum*). 甚至更大胆地, 他引进了记号 α/β 来表示由 $\beta\gamma = \alpha$ 定义的同余类 γ, 同时小心地解释说这并不表示分数, 但是具表示 $(\alpha + np)/\beta$ 的同余类则不一样, 这里 α, β 为它们各自同余类的代表, n 则被选取为使得 $(\alpha + np)/\beta$ 是个整数, 当 β 与 p 互素时这总是可能的 (*Eu.*I-3,521). 对于这一对 $\alpha, 1/\alpha$, 他用的字是 *sociata* (*Eu.*I-3,524), 或者 *socia* (*Eu.*I-3,248), 或者 *reciproca* (*Eu.*I-3,503), 并把这个概念应用到对 -1 模素数 $p = 2n + 1$ 的二次特征标的一个优美的证明上; 证明如下: 注意到, 如果 α 是个二次剩余, 则 $1/\alpha$ 也是, 于是他得出结论说, n 个二次剩余可以重新安排成各个对 $\{\alpha, \alpha'\}$, 其中 $\alpha' = 1/\alpha$ 且 $\alpha \neq \alpha'$ 除非 $\alpha^2 = 1$, 即除非 $\alpha = \pm 1$ (*Eu.*I-3,507,525); 因此, n 为偶数还是奇数由 -1 是在二次剩余中还是不在其中来决定. 当然他也没有忘记这可直接从原根的存在性推导出来; 确实, 如果 r 是这样的一个根, 那么由于 p 除尽

$$r^{2n} - 1 = (r^n - 1)(r^n + 1)$$

但不除尽 $r^n - 1$, 故 r^n 模 p 余 -1; 另一方面, 对于任意 m, r^m 是否是二次剩余根据 m 是否为偶数决定; 从而得到所要结果 (*Eu.*I-3,255,260,262). 按同一脉络, 当欧拉收到拉格朗日的一篇包含了对 "威尔逊定理" 的两个证明的文章 (*Lag.*II,425–438;1771; 参看第二章 §7), 他立即寄给拉格朗日他自己的一个证明, 这个证明根据了如下的观察, 即, 如果 r 是一个模素数 $p = 2n + 1$ 的原根, 则

$$(p-1)! \equiv r^{1+2+\cdots+(p-2)} = r^{n(2n-1)} \equiv (-1)^{2n-1} = -1 \pmod p$$

(*Eu.*IV A-5,496;1773; 参看 *Eu.*I-4,91–93 于 E560;1773).

§3.7 "实" 对 "虚"

在欧拉对模素数的原根的处理 (*Eu.*I-3,249, *Scholion*, 以及 252, 推论 1, E449;1772) 中, 和解与同余式相关联的问题中对 "实 (real)" 和 "虚 (imaginary)" (或 "不可能 (impossible)") 这些字眼的使用不应该在这里不加评论地就忽略过去了. 在十八世纪, 更加特殊地在欧拉那里的使用中, 字眼 "虚" 以两种不同的意思出现; 它或者代表我们所称的复数, 即域 $\mathbb{R}(\sqrt{-1})$ 中的元, 不然的话, 就是某个基域的一个代数扩张中的元, 而这个扩域不能够嵌入到实数域 $\mathbb{R}$ 中; 但这是个那时还没有搞准确的概念, 从而很模糊. 第一种概念受到了十六世纪意大利代数学家关于三次和四次方程工作的启发, 被邦贝利在他 1572 年《代数》的

"书" I 中引进, 很像是模仿了欧几里得的 "书"X 中形如 $a+\sqrt{-b}$ 的无理数理论 (欧几里得的 Campanus的拉丁译本中对此的术语是 "*binomia*, 因而, 邦贝利对复数 $a+\sqrt{-b}$ 的用语也是 "*binomio*"). 进一步的发展已不是数论的事了, 而是属于代数和分析的历史学; 对此只要说欧拉在将重要的分析运算扩充到复数上起了决定性的作用, 这就足够了.

另一方面, 在 1735 年寄给但泽市市长 C.L.G.Ehler 的而实际是让他的同胞, 科学家 H.Kühn 研读的一系列的信 (*PkU*.282–329, 特别地, pp. 297–301,324–328) 中, 欧拉陈述了他关于数的概念的逐次扩张的观点, 首先从普通的数到正的和负的整数, 然后到有理数和到各种 (实的) 无理数, 而超越它们到了代数扩张; 按欧拉的观点, 在每一步全部所需要的是让通常的代数规则应该继续成立, 并且不应引出矛盾; 对于最后的这个观点, 欧拉无疑满足于他自己的和其他有资格的数学家的广泛经验. 按照这个观点, 每一个多项式必须分解为像它次数一样多的线性因式; 例如, 他说 "我决定," ("*iam statuo*": 同上 p.325) x^3-ax^2-bx-c 由三个因式 $x-p$, $x-q$, $x-r$ 组成. 在做出使其满意的例子, 即那个出现两个复根的 $x^3-8=0$ 后, 欧拉没有再举例了, 而 Kühn 的确觉得它如此有说服力, 以致撤回了他的异议.

在欧拉和他的同代人的语言里, 所谓的 "代数基本定理" (用现代术语表示正好是说 $\mathbb{R}(\sqrt{-1})$ 为代数闭) 可以表达为所有代数方程的 "虚" 根均可写成 $a+b\sqrt{-1}$; 如欧拉所知, 一个等价的陈述是说, 每个 (具实系数的) 多项式都可写成次数为一或二次的因式的乘积. 这个问题在积分计算中获得了特殊的重要性, 这是因为用对数和反三角函数的有理函数的积分法依赖于它 (参看下文的 §15). 1742 年欧拉使得自己相信所有的有理函数均可按此方法积分; 但在 1703 年莱布尼茨曾表达了相反的观点 (*Math.Schr.*,ed. C.I.Gerhardt(II)Bd.I.360); 甚至在 1742 年, 尼古拉斯 · 伯努利, 这位欧拉朋友丹尼尔的表兄, 以为他可以提供一个反例, 从而成功地在短时期里动摇了欧拉的信心 (*Corr.*I,170–171; 参看 *Corr.*II,695, 以及欧拉的《*Opera Postuma*》, Petropoli 1862=Kraus Reprint 1969,pp.525–539), 但最后他还是接受了欧拉的论证. 且不问达朗贝尔、欧拉、拉格朗日、高斯的贡献如何, 这件事一直到很久以后也不能说已充分了解了 (从分析上看, 一直到柯西和他的后继者; 从纯代数的观点看, 一直到阿廷 (Artin) 和施雷尔 (Schreier)); 这个故事在这里与我们没有必要的关联.

但是在欧拉关于 m 次剩余的论文 E449;1772 中, 基域是隐含着的素域, 即模素数 p 的整数域 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$. 欧拉称一个同余式 $f(x)\equiv 0 \pmod p$ 的解为 *casus* ("一个案例 (a case)") 或者 *solutio*, 即使得 $f(x)$ 可以被 p 除尽的一个解; 如果 $x=a$ 为这样的解, 则他说所有的值 $a+mp$ 都被算作一个且同一个 "case" ("*pro unico casu*": *Eu.*I-3,249,*Scholion*). 如果 $f(x)=x^{p-1}-1$, 则所有这些 "cases" 都

是"实的";因此如果 $f(x)$ 是任意除尽 $x^{p-1}-1$ 的多项式也同样如此 (*Eu.*I-3,252, 推论 1); 另一方面, 如果 $f(x)=x^n-1$ 且 n 不是 $p-1$ 的因子, 则它们中的一些将是"不可能的"从而"说成是虚的"("*quasi imaginarii*": *Eu.*I-3,249, *Scholion*). 无疑, 欧拉在这里所思考的概念依然具有尚未发展的、模糊不清的形式, 而这些概念是由伽罗瓦在 1830 年引进的, 在它出现的一个时期内被称之为"伽罗瓦虚数", 即模 p 整数域 —— 或另一种说法的有限域 —— 的有限代数扩域的概念.

§3.8 错失二次互反律

整整一生欧拉都深深地涉及整数的表示问题, 先是表为两个平方数之和, 而后则为二次型 (他称其为"公式") X^2+NY^2 或者更一般的 $\mu X^2+\nu Y^2$, 其中 N, μ, ν 为给定整数, 可正可负. 至于形式 $aX^2+bXY+cY^2$, 只在他的暮年时期, 并只在拉格朗日的影响下才涉及, 其实他对它们并不注意 (参看下文的 §9), 但形式 X^2+XY+Y^2 除外, 它不可避免而且悄然地出现在他有关三次剩余和形式 X^2+3Y^2 的研究中 (*Eu.*I-2,572–574 于 E272 中;1759).

这种问题的乘法属性由"婆罗摩笈多 (Brahmagupta) 恒等式"(参看前面第一章 §8, 以及第二章 §12) 清楚显示了出来:

$$(x^2+Ny^2)(z^2+Nt^2)=(xz\pm Nyt)^2+N(xt\mp yz)^2.$$

至少在特殊情形, 欧拉肯定很早就留意到了这个恒等式, 或许与他第一次试图处理佩尔方程及其相关问题有关 (参看 *Corr.*I,36–37;1730,*Eu.*I-2,6–17=E29;1753, 以及下文的 §13), 这是很久以前的事了, 直到后来他才感觉到了将其在 $N=-2$ 的情形弄清楚的必要性 (*Eu.*I-2,237 于 E167 中;1748); 对于 $N=1$ 的最简单情形可参看 *Corr.*I,134;1742, 还有欧拉第一篇关于两个平方数和的论文, 在那里它仍被说成是"值得一提的"的问题 ("*notatu dignum*": *Eu.*I-2,300 与 E228;1749). 一般情形隐含在哥德巴赫写来的一封信里 (*Corr.*I,612;1753) 而在那时欧拉肯定已经知道了它, 在 1755 年 8 月较后的一封信里 (*Corr.*I,629) 它又在一篇关于不定方程的论文里被说成是极端重要的定理 (*theorema eximium*:*Eu.*I-2,660 于 E279 中;1758), 在该文中, 他立刻导出了结论说, 将整数表示为形式 X^2+NY^2 是一个乘法问题, 并首先应该研究一个素数的情形 (同上 p.601).

欧拉知道, 费马处理过 $N=1,2,3$ 的情形并在 1658 年的《*Commercium*》中的信 XLVII 中公布了他的结果 (索引同上, §IV; 参看第二章 §8 和 §12). 但是当欧拉认真着手这些问题时, 他长时间地关注了费马的一个较早时期的陈述, 即, a 和 b 互素时的和 a^2+b^2 没有形如 $p=4n-1$ 的素因子 (*Fe.*II,204=《*Varia Opera*》, p.161; 参看第二章 §7), 从而也没有任何 $4n-1$ 的因子, 不管是否为素.

显然它给了欧拉深刻的印象; 很早以前 (“*vor langer Zeit*”:*Corr.*I,107;1741; 参看 *Corr.*I,114;1742) 他就已将它转换成了如下的陈述, 即, 如果 m, n 为正整数, 那么 $4mn-m-1$ 和 $4mn-m-n$ 都不会是平方数; 的确, 如果 $4mn-m-1$ (分别地, $4mn-m-n$) 是个平方数 a^2, 这就意味着

$$m(4n-1)=1+a^2, \text{分别地} \quad (4m-1)(4n-1)=1+4a^2,$$

故而 $4n-1$ 就会除尽两个互素的平方数的和.

因此欧拉面对了不仅是一种而是三种类型的问题, 对于任意已知的整数 N (正或负, 但不为 0 或 -1), 可以将它们阐明如下:

(i) 哪些是可以写成形如 a^2+Nb^2 的素数, 其中 a 和 b 是整数?

(ii) 形式 X^2+NY^2 的 “素因子” 是什么样的? 在这里我们像欧拉那样, 将它理解为某个整数 a^2+Nb^2 的 (不一定与 N 互素) 奇素因子, 而这里的 a 与 Nb 互素.

(iii) 哪些奇整数是某个整数 a^2+Nb^2 的因子, 其中 a 与 Nb 互素?

欧拉必定很快意识到了, 满足 (iii) 的整数 (与 $2N$ 互素) 正好使得 $-N$ 模它是个二次剩余 (参看 *Eu.*I-2,209, *Annot.*9,219, *Annot.*18, 于 E164 中; 1744; 还可参看《*Tractatus*》,no.300, *Eu.*I-5,229–230). 事实上, 如果 $a^2+Nb^2=mn$, 其中 a 与 Nb 互素, 则 a 和 Nb 必定与 m 互素; 于是存在 b' 使得 $bb'\equiv 1 \pmod m$ (参看前面的 §5 (a)) 从而我们有 $-N\equiv(ab')^2 \pmod m$. 又, 立即可知其逆为真. 例如, 如果 $N=1$, 这便表明 (ii) 的答案必定等价于确定 -1 模任意奇素数的二次剩余特征标 (参看前面的 §4 以及第二章 §7). 如果为简便引进勒让德记号 (n/p), 其定义为: 凡是 p 为奇素数, n 与 p 互素, 那么根据 n 为模 p 二次剩余还是非剩余决定它为 $+1$ 还是 -1 (参看第四章 §6), 于是 (ii) 等于是要求对所有的不除尽 $2N$ 的素数 p 确定 $(-N/p)$. 另一方面, 从二次域理论的观点看, (i) 与 (ii) 等于是探寻一个有理素数 p 在域 $\mathbb{Q}(\sqrt{-N})$ 中的行为: 如果它除尽 a^2+Nb^2, 其中 a 与 Nb 互素, 则在此域中它分解为素理想因子 $(p, a\pm b\sqrt{-N})$; 如果那些因子为主理想 $(a\pm b\sqrt{-N})$, 则它满足 (i). 因此 (i) 要比 (ii) 藏得更深一些; 用欧拉对此的话说, 它是 “*altioris indaginis*” (*Eu.*I-2,603 于 E279 中;1758); 它依赖于二次域中的理想类的理论, 或等价地, 二元二次型的理论, 然而 (ii), 我们将在后面看到 (参看附录 I), 不过依赖于二次互反律罢了.

成年累月, 欧拉孜孜不倦地探索着以上问题的方方面面, 并且将他可能收集到的有关它的哪怕一点点信息都集中起来. 在 1741 年我们发现他向哥德巴赫介绍他所发现的关于 X^2-2Y^2, X^2-3Y^2, X^2-5Y^2 的 “奇特的性质 (*curieuse proprietates*)(*Corr.*I,107;1741 年 9 月 9 日); 在后一种情形中, 这已经超过了费马所有陈述过的. 在下一年, “*curieuse proprietates*” 便成长为 “非常美艳的布

局" ("*eine sehr artige Ordnung*": *Corr.* I,146; 1742 年 8 月 28 日), 他立即在他的实验基础上开始描述它, 同时预言说这只不过是尚待发现的更加 "辉煌的性质" ("*herrliche proprietates*": 同上, p.150) 的先奏罢了. 不迟于 1744 年 ("*vor einiger Zeit*": *Corr.*I,279;1744 年 7 月 4 日) 他将关于 X^2+NY^2 的素因子的, 他的所有经验性观察结果 (涵盖了 N 的 16 个正值和 18 个负值), 并加上理论性的结论, 以一系列《评注 (*Annotationes*)》的形式汇拢一起, 全部递交给了彼得堡. 这就是论文集 E164(=*Eu.*I-2,194–222), 彼得堡科学院在 1751 年将其发表.

从这里开始我们将假设 N 为无平方因子的整数; 只要涉及 (ii) 和 (iii), 这对一般性并没有任何限制. 在现代的术语和记号下, (ii) 的答案最好用相伴于域 $\mathbb{Q}(\sqrt{-N})$ 的 " 狄利克雷特征标" 来描述. 这是一个整数的周期函数 ω, 取值 ±1 和 0, 其周期 D 为: 如果 $N\equiv-1 \pmod 4$, 则 $D=|N|$, 否则 $D=4|N|$; 它使得素数 p 满足 (ii) 当且仅当 $\omega(p)=1$; 换句话说, 对所有不除尽 $2N$ 的素数 p 我们有:

$$\omega=\left(\frac{-N}{p}\right).$$

在附录 I 中将给出 ω 的一个构造以及充分的特征描述.

设模 $4|N|$ 的、并与 $4|N|$ 互素的同余类中使 ω 在其上取值为 1 的那些类的集合为 K_N; 因此一个素数满足 (ii) 当且仅当它的模 $4|N|$ 的同余类属于 K_N. 我们将在附录 I 中看到, K_N 可以由以下的性质作特征描述:

(A) *K_N 是模 $4|N|$ 乘群的一个指数 2 的子群.* 这表明它包含了所有模 $4|N|$ 且与 $4|N|$ 互素的二次剩余.

(B) *-1 是否属于 K_N 由 $N<0$ 还是 $N>0$ 决定.*

(C) *K_N 具有周期 D, 但不具有周期 $D'<D$.* 这表明, 如果 r 和 s 与 $4|N|$ 互素且 $r\equiv s \pmod D$, 则只要两个中有一个属于 K_N, 那么两个都属于它, 并且没有 D 的因子 $D'<D$ 具有这同一个性质.

K_N 的这个特征描述因而可以看作是提供了对 (ii) 的一个完全回答.

基于他的实验数据的第一个重要发现是, 观察到 X^2+NY^2 的素因子正好是那些属于一些确定的算术级数

$$P(r)=\{r,4|N|+r,8|N|+r,\cdots\}$$

中的素数, 其中 r 与 $4|N|$ 互素且 $0<r<4|N|$ (索引同上, *Annot.*3,13; 参看 *Corr.*I,147; 1742).

这里要记住狄利克雷定理, 根据它每个像 $P(r)$ 那样的级数包含了无穷多个素数; 如果不是这样, 欧拉的实验就不会进行得如此成功. 因此, 由具上面性质的 $P(r)$ 中 r 所决定的模 $4|N|$ 的同余类的集合恰好就是前面引进的 K_N.

欧拉写信给哥德巴赫说, 最初看来, 似乎在构成集合 K_N 的数中没有什么规则 (“*keine Ordnung*”: *Corr.*I,147); 然而它们却依照 “一个漂亮的法则” (“*nach einer schönen lege*”, 这是他所写的德文和拉丁文的混合体: 索引同上) 在运行. 首先, 所有 K_N 中的元的幂和幂的乘积仍然属于 K_N (*Corr.*I,148,150;*Annot.*8,16); 用我们的话说, 这表明 K_N 是模 $4|N|$ 乘群的一个子群. 因为显然地, 每个满足 (iii) 的整数是满足同一条件的素数和素数幂的乘积, 这表明了这个重要事实, 即所有这样的整数也必须属于某个 $P(r)$, 其中的 r 属于 K_N (参看索引同上, pp. 220–222, Scholion,2,3), 也许就是这使得欧拉发现了 K_N 的群性质. 同样的说法特别证明了所有奇整数 a^2+Nb^2 必定属于某个 $P(r)$, 其中 r 在 K_N 中, 同时 a 与 Nb 互素; 对于 $b=2$ 以及 a 与 $2N$ 互素, 他证明了所有的模 $4|N|$ 的二次剩余属于 K_N (*Annot* .7,16). 再者, 如果 r 属于 K_N, 那么若 $N<0$, 则 $-r$ 也属于 K_N, 但 $N>0$ 则不是如此 (*Annot.*3,13); 另外, K_N 中元素的个数是模 $4|N|$ 且与 $4|N|$ 互素的同余类个数的一半(*Annot* .5,14) 即 $\frac{1}{2}\varphi(4|N|)$, 其中 φ 是 “欧拉函数”. 因此欧拉发现了 K_N 具有以上列出的性质 (A) 和 (B).

至于 (C), 欧拉告诉我们说, 如果 r 属于 K_N, 则 $r+2|N|$ 对于 $N\equiv -1 \pmod 4$ 也属于它 (*Annot.*11,19), 否则便不如此 (*Annot.*12,20). 这意味着, 在前一种情形, K_N 具有周期 $|N|$; 事实上, 如果 r 和 s 都与 $4|N|$ 互素, 那么他们则均为奇数, 故而, 如果 $r\equiv s \pmod{|N|}$, s 必定是 $\equiv r$ 或者 $\equiv r+2|N| \pmod{4N}$. 有鉴于此以及欧拉的特殊提及的一个事实, 即对于 $N\equiv 1$ 或 $2 \pmod 4$ 它不再成立, 我们于是可以推测他的确曾寻找过别的周期; 如果我们相信他已经感觉到了没有这样的周期, 我们或能得出结论说, 他已经获得了 (当然只是猜测) 集合 K_N 全部的特征, 从而得到了问题 (ii) 的完全答案.

有赖于此, 欧拉远远地漫步在费马曾行走过的道路的前方. 隐藏在他的猜测之中的, 或许作为他宝藏中最有价值的金块, 躺着二次互反律 (参看附录 I, 以及前面的 §5(i)), 可惜, 直到生命的很后期之前他一直也没能认识到此. 他甚至曾有过机会把他的实验推向更远的地方; 在他为《*Tractatus*》写具高度尝试性的关于三次和双二次剩余的章节时, 他寻找了对于 2, 3, 5, 6, 7, 10 成为模素数 p 的二次剩余和 2, 3, 5 成为模素数 p 的双二次剩余的条件 (*Eu.*I-5,250–251, no.407–410, 以及 258–259,no.456–457). 至于后面这个问题, 它只在 $p\equiv 1 \pmod 4$ 时发生, 这是因为否则的话, 如欧拉注意到的 (同上 p.252, no.419), 每个二次剩余就会是一个双二次剩余; 因此欧拉可以写出 $p=a^2+4b^2$, 从而发现 2, 3 还有 5 的模 p 双二次特征标只依赖于 a 和 b 分别模 4, 模 6, 模 5 的值. 相似地, 对于三次剩余, 只需考虑 p 可以写成 $p=a^2+3b^2$ 的情形就够了, 于是按照欧拉所正确叙述的方式知, 2, 3, 5, 7, 还有 10 的三次剩余特征标只分别依赖于 a 和 b 的模 3, 模 9, 模 15, 模 9, 模 21, 和模 5 的值. 这些辉煌但完全孤立的观察到的结果已消失在数

学世界里了; 在 1849 年当《 *Tractatus* 》首次出版时, 高斯而后雅可比, 还有艾森斯坦, 已经证明了所有欧拉猜测的东西, 当然还要更多 (参看 *Eu.*I-5,pp.21–24).

§3.9　二元二次型

1741 年到 1744 年间, 在把有关形式 X^2+NY^2 的素因子的实验数据汇集的同时, 欧拉寻求使用他的结论以便推广他较前关于整数 $4mn-m-n$ 不是平方数的注记. 例如, 在他写给哥德巴赫的信中说道 (*Corr.*I,162;1742 年 10 月 27 日), 由于他的观察表明了形式 X^2+NY^2 对 $N>0$ 没有因子 $r=4Nx-1$, 于是整数 $4Nmn-m-n$ 对于正的 m, n 不会是平方数; 事实上, 如果他等于 a^2, 那么这就会给出

$$(4Nm-1)(4Nn-1)=1+4Na^2.$$

他补充道, 或许后面的这个陈述比前面的那个更容易证明 (同上; 参看 *Corr.*I,179; 1743 年 1 月 5 日). 从 1741 年到 1744 年, 欧拉和哥德巴赫这两个朋友之间的几乎所有通信都涉及这个课题; 甚至在他的 1744 年的学术报告中也在最后面包含了一列的 "公式" $4Nmn-A(m\pm n)$, 其中的值, 由他的观察, 对于 m 和 n 为正且与 A 互素时绝不是一个平方数 (*Eu.*I-2,220–222; 参看 *Corr.*I,260,278). 终于他明白必须放弃他寻找对这种陈述的直接证明的希望了. 然而观察哥德巴赫为证明其中最简单的一个情形的顽强努力是有趣的, 这是与 $4mn-m-n$ 有关的一个情形, 即便如此, 从欧拉的证明的观点看来这也是不必要的 (1742 年 3 月 6 日寄给哥德巴赫的信, 并在 1743 年 1 月 19 的信中又重复了一遍 *Corr.*I,115–117,191–192); 这是要证明 X^2+Y^2 没有形如 $p=4n-1$ 的素因子. 带着点从欧拉来的激励和一点帮助, 哥德巴赫终于成功了 (*Corr.*I,255-256;1743 年 9 月 28 日); 他的证明或许是在整个通信中唯一有价值的贡献吧; 他使用了下降法; 但愿他和欧拉能够知道, 它包含了对二元二次型的拉格朗日简约理论的最初萌芽 (见下文).

除了这一段已经走入死胡同的故事外, 欧拉多年来一直集中精力在证明费马关于 "初等形式" 的陈述, 这里指的是形式 X^2+NY^2, 其中 $N=1,\pm2,3$, 它们对应了具有欧几里得算法的域 $\mathbb{Q}(\sqrt{-N})$ (参看第二章 §8,§9 以及附录 I); 在这些域中, 如通常算术中那样, 整数可以分解为素因子, 故而像 X^2+NY^2 这种形式的每个素因子均可用它来表示; 换句话说, §8 的问题 (i) 的答案与对 (ii) 的答案是一样的. 这些事实已经由费马陈述并推测性地被他证明; 欧拉不得不重新构造证明, 这花了他许多年.

在这方面的第一个步骤是处理对形式 X^2+Y^2 的 (ii) 的较容易的部分, 证明没有素数 $p=4n-1$ 可以是这个形式的因子, 或者换句话说, 对那样的素数 p

有 $(-1/p)=-1$; 这是费马定理 $a^{p-1}\equiv 1 \pmod p$ 的一个直接推论 (*Corr.*I,115–117;1742; 参看第二章 §6). 决定性的进展出现在 1747 年, 仍然是对 $N=1$ 的; 在一封给哥德巴赫的信 (*Corr.*I,416–417) 中, 欧拉叙述了他新近发现的证明; 这是在第二章 §8 中再现的那个证明; 关键的引理[5] (第二章 §8 的引理 2) 在该信中作为定理 2 出现. 因此证明了, X^2+Y^2 的每个素因子都可写成 a^2+b^2 并因而具有 $p=4n+1$ 的形式.

还需要证明每个素数 $p=4n+1$ 都是 X^2+Y^2 的一个因子, 即对这样的素数 p 有 $(-1/p)=1$; 如我们已知道的那样, 这个断言的证明已在 1749 年完成 (参看前面 §5(b),§6). 至于 1747 年的信, 它的内容的一部分几乎逐字逐句地写到欧拉关于两个平方数和的第一篇学术报告中了 (*Eu*,I-2,295–327=E228;1749), 可惜包含了其论证最后部分的十分粗心的和不完善的表述. 跟随其后的是 1753 年对于形式 X^2+2Y^2 的一个非常清晰的处理, 用的却是同一个方法 (*Eu*.I-2,467–485 于 E256 中;1753), 以及 1759 年对于它到 X^2+3Y^2 的推广 (*Eu*.I-2,556–575=E272;1759; 参看 *Eu*.I-2,481–482 于 E256 中;1753); 对这些情形的证明从本质上说就是在第二章的 §12 所叙述的那些.

因此已经证明了 X^2+NY^2 对于 $N=2$ 或 3 的每个素因子都可以写成 a^2+Nb^2, 从而对于 $N=2$ 必为 $\equiv 1$ 或 $3 \pmod 8$, 对于 $N=3$ 为 $\equiv 1 \pmod 3$; 欧拉还证明了它们的逆. 对于 $N=3$, 欧拉于 1759 年完成了证明 (*Eu*.I-2,573 与 E272 中;1759, 命题 9); 这个证明我们已将其重现于第二章 §12, 它基于的是恒等式

$$x^{3n}-1=(x^n-1)(x^{2n}+x^n+1).$$

在对该证明的 *Scholion*(评注) (索引同上,p.575) 中, 欧拉提到他也知道如何证明一个素数 $p=8n+1$ 是 X^2+2Y^2 的素因子 (但不是证明对于 $p=8n+3$ 的); 无疑他在这里暗指的是在 1772 年所发表的一个证明, 我们已将其重现于第二章的 §12; 它基于的恒等式为

$$x^{8n}-1=(x^{4n}-1)[(x^{2n}-1)^2+2x^{2n}]$$

(*Eu*.I-3,274–275 于 E449 中;1772,no.85). 然而他通过 “与一个朋友的交流” (可能是 Lexell) 知道, 这后面的文章还可以走得更远; 事实上, 这位朋友仅仅指出了欧拉对于证明 X^2+2Y^2 的每个素因子均可写成 a^2+2b^2 形状的论证对于 X^2-2Y^2 仍旧有效 (索引同上, p.275; 参看 *Eu*.I-3,183 于 E427 中;1772). 因此一个素数 $8n+3$ 不可能是 X^2-2Y^2 的因子, 故对于这样的一个素数我们有 $(2/p)=-1$; 由于我们有 $p\equiv 3 \pmod 4$, 那么它表明了 $(-1/p)=-1$, 从而得到 $(-2/p)=1$, 即

[5] 无疑这个更一般的陈述 “如果 ab 和 a 是两个平方数之和, 则 b 也是” 是过于超前了, 尽管欧拉断言他能够十分严格地 (*rigidissime*) 证明它.

我们要证明的 (参看第二章的 §12). 这便完成了对于所有奇素数 p 确定 $(\pm 2/p)$ 的任务, 这是因为它证明了 $(-2/p)$ 等于 1 当且仅当 $p \equiv 1$ 或 3 (mod 8) 并且由于 $(-1/p)$ 已知的缘故. 顺便提下让人好奇的一件事, 就在我们刚刚提到的同一天里向彼得堡科学院提交的一篇文章 (*En.*I-3,511 于 E552 中;1772,*Scholion* 3; 也可参看 *Eu.*I-4,38 于 E557 中; 1773,no.24–25) 中, 欧拉或者无论哪个为他听写的人, 好像没有留意到对于 $p = 8n+3$, $(-2/p) = 1$ 的结果已经刚刚证明过了. 或许在那个时候, 欧拉的文章有时只不过是与他的助手们交谈的记录罢了.

因此, 在 1772 年, 欧拉在有关形式 X^2+Y^2, $X^2 \pm 2Y^2$, X^2+3Y^2 的素因子问题方面, 以及用这些形式表示整数方面, 已全面赶上了费马. 他有一个方面超越了费马, 这是一个吸引了拉格朗日注意力的、并在以后被高斯广为推广的一个观察结果 (参看下文的第四章 §6). 高斯证明了, 如果 p 是个奇素数, 则 $\sqrt{\pm p}$ 包含在 p 次单位根域中, 这里的符号由使 $\pm p \equiv 1 \pmod 4$ 决定. 这表明 "分圆多项式" $X^{p-1}+X^{p-2}+\cdots+1$ 在域 $\mathbb{Q}(\sqrt{\pm p})$ 中分解, 故而有两个 $\frac{1}{2}(p-1)$ 次整系数的齐次多项式 $F(X,Y)$, $G(X,Y)$, 满足恒等式

$$4(X^{p-1}+X^{p-2}Y+\cdots+Y^{p-1}) = F(X,Y)^2-(\pm p)G(x,Y)^2.$$

例如, 对于 p, 可以取 $F = 2X+Y$, $G = Y$, 而这是欧拉在处理 X^2+3Y^2 时的主要构成部分. 相似地, 如果 $q = pn+1$ 也是个素数, 那么对于 $X = a^n$, $Y = b^n$ 给出了

$$4(a^{q-1}-b^{q-1}) = (a^n-b^n)[F(a^n,b^n)^2 \mp pG(a^n,b^n)^2],$$

用在 $p = 3$ 情形相同的论证, 它表明了 $\pm p$ 是个模 q 的二次剩余. 欧拉对于 $p = 5$ 和 $p = 7$ 情形进行了运作 (*Eu.*I-3,280–281 于 E449 中;1772,no.96–97); 不久后拉格朗日也做了, 但他在试图将其拓展到 $p = 11$ 时没有成功 (*Lag.*III,789–792;1775).

至于用形式 X^2+NY^2 的素数表示问题 (§8 中的问题 (i)), 对于除了费马考虑过的之外的其他 N 值, 欧拉长时间中停留在满足于他放进了 1774 年学术报告中的实验结果. 1742 年, 在向哥德巴赫通告了我们在 §8 中叙述过的 "辉煌性质" 后, 他便已经简单地涉及了这个问题, 轻率地宣称 X^2+NY^2 的每个素因子都可以表示为这种形式, 并举出 N 的下面情形作为例子: $N = 1,2,3,7$ (这是对的), 还有不正确的 $N = 5,6$ (*Corr.*I,146–148). 1743 年他仍然以为, 如果一个素数 p 是个模 $4N$, $N > 0$ 的二次剩余, 则它就可以写成 a^2+Nb^2 (*Corr.*I,264). 在他的 1744 年的学术报告中, 他放进了一组关于 12 个正 N 值以及 $N = -2,-3$ 值的实验发现; 我们将其作为典型例子引述于后:

1° 如果 p 是 X^2+5Y^2 的一个素因子, 则对 $p \equiv 1$ 或 9 (mod 20) 它可写成 a^2+5b^2; 对于 $p = 3$ 或 7 (mod 20), $2p$ 也可写成这样 (*Eu.* I-2,196, 定理 11).

2° X^2+7Y^2 的所有素因子都可写成 a^2+7b^2 (索引同上, p.197, 定理 14).

3° 如果 p 是 X^2+17Y^2 的一个素因子, 则当 p 为模 $4\times 17=68$ 二次剩余时, p 或 $9p$ 可以写成 a^2+17b^2; 否则, $3p$ 可写成这样 (索引同上, p. 199, 定理 23).

4° 如果 p 是 X^2+14Y^2 的一个素因子, 则当它 $\equiv \pm 1 \pmod 8$ 时, 它可写成或者 a^2+14b^2, 或者 $2a^2+7b^2$; 否则, $3p$ 可写成这样 (索引同上, p.203, 定理 35).

他必定感觉到这些现象所带来的困惑; 甚至十年之后在一篇颇有意味地冠以 "*Speimen de usu observationum in pura mathematica*" ("论观察在纯数学的使用": *Eu.*I-2,459–492=E256;1753) 的大体上致力于处理形式 X^2+2Y^2 的论文中, 他重复他较早的一些陈述, 评述道:"它们似乎是确定的但又确实十分难于证明" (索引同上, p.486). 在同一年他向哥德巴赫指出, 一个素数 $p=4Nx+1$ 可不必由形式 X^2+NY^2 "*in integris*" 表示, 即表示为 a^2+Nb^2, 其中 a 和 b 为整数; 虽然如此, 他仍然笃信 (而且是正确地相信了; 参看第四章的附录 I) 它总可以有理地如此表示 ("*in fractis*": *Corr.*I,605–606;1753); 换句话说, 方程 $p=x^2+Ny^2$ 即便没有整数解, 也必有有理解. 1772 年, 他递交给科学院一篇论文 (*Eu.*I-4,1–24=E556), 它是关于可以由二次型 $\mu X^2+\nu Y^2$ 有理表示的整数的; 但除了一些包含二次型复合的一些特殊情形的公式外, 这里没有什么新东西 (p.2, 定理 1, 和 p.4, 定理 2; 参看第四章 §6), 更不必提及解方程 $ax^2+by^2+cz^2=0$ 的拉格朗日方法 (参看第二章 §14, 和第四章 §2) 的令人困惑和乱糟糟的变异版本了 (pp.18–24); 令人惊讶的是, 虽然拉格朗日的文章 (*Lag.*II,377–535;1768) 曾有一段时间就放在欧拉那里, 欧拉也曾在一封给拉格朗日的信里对此有所评论 (*Eu.*IV A-5,466;1770 年 1 月 16 日), 他却没有在那里提及此事.

除了这一件令人困惑的事外, 没有迹象表明欧拉关于这方面取得了任何进展, 这种情况一直延续到 1775 年, 那时他从拉格朗日那里收到连同一本《都灵杂记 (*Miscellanea*)》一起的还有包含了拉格朗日的《算术研究 (*Recherches d'Arithmétique*)》(*Lag.*II,III,695–758;1775) 的一卷柏林 "学术论文集 (*Mémoires*)". 在将此送给欧拉时, 拉格朗日以他通常缺少自信心的状态表达了他是多么热切地期待着欧拉对他最新工作的裁决:

"*Si vos occupations et l'etat de votre santé vous ont permis de jetter les yeux sur le peu que j'ai donné dans les Memoires de Berlin et de Turin, je vous supplie de vouloir bien m'en dire votre avis; ma plus grande ambition a toujours été d'obtenir votre suffrage...*" ["如果您的工作和您的健康状态允许您能看一下我对此卷所作的一小点贡献的话, 我恳求您给我您对它们的意见; 我最大的雄心一直是能赢得您的首肯……": *Eu.*IV A-5,503–504;1775 年 2 月 10 日].

任何责备他伪善, 或者怀疑他沽名钓誉, 都是错误的 (参看第四章 §2). 无论怎样, 欧拉以前所未有的热情对他的工作表示了祝贺:

他写道:"*Il est bien glorieux pour moi, d'avoir pour successeur à Berlin le plus sublime geomètre de ce siecle...J'ai parcouru avec la plus grande avidité les excellens mémoires dont vous avés enrichi les derniers volumes de Berlin et de Turin...*"["由本世纪最杰出的数学家作为我的柏林继任者, 这是对我最大的奉承…… 我已经热心地通读了您对当前一卷所做的卓越贡献……":*Eu.*IV A-5,504=*Lag.*XIV,241;1775 年 3 月 23 日]. 在那一封信里他并没有专门提到《*Recherches*》; 但是在几个月里他写出了题目是 "*De insigni promotione scientiae numerorum*" ("关于数的科学的一些著名的进展") 的文章:*Eu.*I-4,163–196=E598; 1775), 这是一种对于学术论文进行评论的文章, 并于 1775 年 10 月 26 日呈交给了科学院. 在他身后的 1785 年方才出现.

与许多伟大的发现没有什么不同, 拉格朗日的基本思想本身是简明的; 他在对欧拉的《代数学》的 "*Additions*(附件)" 中对此已有叙述 (*Lag.*VII,125–127=*Eu.*I-1,603–605,no.70); 但是在那时欧拉虽然承认 (相当敷衍了事地: *Eu.*IV A-5,496=*Lag.*XIV,236;1773) 收到了那卷书, 但却没有注意到这个闪亮的思想. 在 1775 年的《*Recherches*》里它占用了 4 页 (索引同上, pp,697–700); 在当前来说, 下面的叙述就足够了. 如果 $-N$ 是模一个整数 e (不必是素数) 的二次剩余, 那么, 当记 $-N = f^2 - eg$ 时, 我们便看出 $-4N$ 就是二次型 $F(X,Y) = eX^2 + 2fXY + gY^2$ 的所称作的 "判别式", 并且 $F(1,0) = e$ (一般地, 一个形式 $aX^2 + bXY + cY^2$ 的判别式定义为 $\delta = b^2 - 4ac$). 欧拉写道 "由此似乎并没有增加多少东西" ("*parum hinc lucri ad nostrum institutum afferri videtur*": 索引同上, p .165), "如果是这样, 那就不能解释拉格朗日的发现, 即具有判别式 δ 的无穷多个形式" ("*infinitam...formularum multitudinem*") 对于每个 δ 可以化为一个 "小的数"(*ad exiguum numerum*"). 事实上, 考虑形式

$$F(X,Y) = aX^2 + bXY + cY^2,$$

其判别式为 $\delta = b^2 - 4ac$; 这里我们仅仅假定 δ 不是 0 也不是平方数; 特别我们假定 $ac \neq 0$. 假设 $|a|$ 或者 $|c| < |b|$; 于是如果 $|b| > |a|$ 则用 $X - rY$ 替换 X (分别地, 如果 $|b| > |c|$ 则用 $Y - rX$ 替换 Y), 并适当选取 r, 我们可以得到形式

$$F_1(X,Y) = a_1X^2 + b_1XY + c_1Y^2,$$

它具有相同的判别式 δ, 但其中 $|b_1| \leq |a| < |b|$(分别地, $|b_1| \leq |c| < |b|$), 故无论如何都有 $|b_1| < |b|$. 显然 F 和 F_1 在它们 "正常表示" 同一个整数的意义下是 "等价" 的; 这个意思是说, $F(\alpha,\beta)$ 当 α 与 β 互素时所取值的集合与 F_1 的那样

的集合一样 (更多的细节参看第四章 §4), 无疑 "拉格朗日简约" 的从 F 推导出 F_1 的过程是可以重复的, 然而最多是有限次, 这是因为 $|b|$ 在每一步都在减小, 直到到达了形式

$$\phi(X,Y) = pX^2 + qXY + rY^2,$$

它仍旧等价于 F 并仍旧具有同一个判别式 $\delta = q^2 - 4pr$, 并对此 ϕ 有 $|p|$ 和 $|r|$ 都 $\geq |q|$. 简单的计算表明当 $\delta < 0$ 时, $q^2 \leq \frac{1}{3}|\delta|$, 而当 $\delta > 0$ 时, $q^2 \leq \frac{1}{5}\delta$; 由于 $4pr = q^2 - \delta$, 这表明对于给定的 δ 只有有限个这样的形式 ϕ. 此外, 因为 $a = F(1,0)$, 我们必有 $a = \phi(\alpha,\beta)$, 其中 α 与 β 互素, 因此

$$4pa = 4p(p\alpha^2 + q\alpha\beta + r\beta^2) = (2p\alpha + q\beta)^2 - \delta\beta^2.$$

如果对于给定的一个 δ, 将所有满足上述条件的这种形式 ϕ 列出来:

$$\phi_i = p_iX^2 + q_iXY + r_iY^2 \quad (i = 1, 2, \cdots, m),$$

这表明这些整数 $4p_ia$ 中有一个由 $X^2 - \delta Y^2$ 表示.

新的问题是, 是否为此需要全部这些 ϕ_i? 拉格朗日已经充分考虑到了这一点 (索引同上, pp.723–740; 参看第四章 §4 以及附录 II,III). 欧拉没有提到它; 或许他觉得它没有多少意思, 要么就是拉格朗日为解决该问题而作出的精心计算远不是失明了的欧拉所能理解的.

特别地, 像前面那样取 N 无平方因子, 并仍设 e 为 $X^2 + NY^2$ 的一个因子, 即一个正整数使得 $-N$ 为一个模 e 的二次剩余. 令 $-N = f^2 - eg$ 并应用前述的 "拉格朗日简约" 到具有判别式 $\delta = -4N$ 的形式

$$F(X,Y) = eX^2 + 2fXY + gY^2$$

上; 设 ϕ 如前, 我们有 $q^2 - 4pr = -4N$, 故 q 为偶. 记 $e = \phi(\alpha,\beta)$, 现在得到了

$$pe = \left(p\alpha + \frac{q}{2}\beta\right)^2 + N\beta^2.$$

因此, 如果我们仍旧记 $\phi_1, \cdots, \phi_m$ 为对判别式为 $\delta = -4N$ 的那些 ϕ, 使得每个整数 p_ie 都可由形式 $X^2 + NY^2$ 表示. 举 $N = 1$ 为例; 于是这里除了 $\phi_1 = X^2 + Y^2$ 外再没有其他的 ϕ 了 (忽略掉 $-\phi_1$, 因为它不取正值); 因此那个形式的每个因子都可由它表示, 特别地, $X^2 + Y^2$ 的每个奇因子均为 $\equiv 1 \pmod 4$. 本质上说, 这只不过是哥德巴赫在 1743 年精心炮制的那个证明罢了.

这个例子提示我们, 欧拉的许多老的猜想现在可以由上面的结果推导出来; 其中一些在拉格朗日的《*Recherches*》中已有处理; 更多的则添加进了 1777 年发表的论文的续篇之中 (*Lag.*III,759–795;1775). 作为进一步的例解我们可以举出

$N = 5$, $\delta = -20$ 的情形. 这里我们有了形式 $\phi_1 = X^2 + 5Y^2$, $\phi_2 = 2X^2 \pm 2XY + 3Y^2$; 因此, 如果 p 是 $X^2 + 5Y^2$ 的一个奇素因子, 它或者可写成 $p = a^2 + 5b^2$, 这时 $p \equiv 1$ 或 $9 \pmod{20}$, 要么 $2p$ 可以写成这样, 这时 $p \equiv 3$ 或 $7 \pmod{20}$. 这个论证不能用于证明它的逆, 这是欧拉发现该形式的另一方面, 这就是, 每一个素数 $p \equiv 1, 3, 7, 9 \pmod{20}$ 都是 $X^2 + 5Y^2$ 的因子. 然而欧拉是高兴的, 非常乐于对拉格朗日的发现添加许多例子, 或者更恰当地说, 是由他的助手做出来的例子.

在实质上超越了拉格朗日新方法范围的仍是二次互反律. 欧拉在他的老年至少成功地把它从他的早期各种猜想中剥离出来; 这构成了他 1772 年关于二次剩余文章的结论 (*Eu.*I-3,510–512 于 E552 中;1772). 他对它的表达, 如使用两个奇素数 p 和 s 的话, 等于是写出了关系式

$$\left(\frac{s}{p}\right) = \left(\frac{\pm p}{s}\right),$$

其中的符号是按照 $\pm p \equiv 1 \pmod 4$ 取的 (参看附录 I). 1773 年, 他又一次吸引了拉格朗日对于这类事情的注意; 他写道或更确切地, 口授道:"*Je suis fort assuré que la considération de ces circonstances pourra conduire à des découvertes très importantes*"["我确信它将导致非常重要的发现":*Eu.*IV A-5,498=*Lag.*XIV,238;1773]. 在上面所描述的他 1775 年的学术报告中, 处理了拉格朗日的简约理论之后, 他指出了这个是如何部分肯定了他从前的猜测的, 并得出结论说 "因此所有我曾很久以前在老的 [彼得堡] 《*Commemtarii*》vol. XIV 中阐述的 '定理' 已经取得了很高程度的确认…… 而且似乎肯定它们中还有点什么仍然值得期待的东西也将会很快得到完全的证明" ["*Nunc igitur omnia theoremata, quae· · · olim in Comment.veter.Tomo XIV dederam, multo maiorem gradum certitudinis sunt adepta...atque nullum dubium esse videtur,quin mox,quod in hoc genere ashuc desideratur, perfecta demonstratione muniatur*": *Eu.* I-4,195 于 E598 中;1775].

他说的不算错. 但是在那些年代里数学不像今天那样, 那时它迈着十分悠闲的步履向前走着. 证明二次互反律仍需花二十多年; 要由高斯来做成它.

§3.10 搜寻大素数

费马曾说过, 不仅每个素数 $p = 4m + 1$ 是两个平方数的和, 而且它以一种唯一的方式写成这种表示; 从而对此的逆可以容易地从他的关于此课题的进一步的陈述中提取出来 (参看第二章 §8,§9). 因此那些结果暗含着对一个整数 $4m + 1$ 为素数的判别法.

在能够证明它的很久以前, 欧拉就已留意到此了. 1742 年, 他写信给哥德巴

赫说, $4m+1$ 是个素数当且仅当它可以一种且唯一的一种方式 (“*unico modo*”: *Corr.*I,134–135) 写成 a^2+b^2, 并用 “费马数” $2^{2^5}+1$ (自 1732 年起他就知道它不是个素数; 参看 §4) 对它作了例解, 它的确可以写成

$$(2^{16})^2+1=62264^2+20449^2.$$

在他的第一篇关于两个平方数之和的论文里, 欧拉描述他较早时的断言为, $4m+1$ 为素数 “当且仅当它可以一种且只有一种方式写成 a^2+b^2, 其中 a 与 b 互素” (*Eu.* I-2,314 于 E228;1749). 因此, 如果我们又称一个整数 n 以两个平方数和的表示 $n=a^2+b^2$ 为 “正常的” 是说 a 与 b 互素的话 (参看前文第二章 §9), 那么欧拉看起来是在说, 如果 $4m+1$ 具有一个这种和的正常表示则它是个素数. 他的表达没有一个是准确的; 他必定已经知道, $45=36+9$, $25=16+9$, $125=121+4$ 给出的反例. 按照他那个年代的风尚, 他必定将这样的例外看作是 “证明的规则”, 或者不如说看作是仅仅出现在那些显然不值得提及的情形. 十分准确地, 他所说的应该是: 一个 $m>0$ 的整数 $4m+1$ 为素数当且仅当它具有一个且只有一个两个平方之和的表示, 而且那个表示是正常的; 在这个陈述中, 人们必须将 a^2+0^2 看作是 a^2 的一个表示, 但不是一个正常的表示.

在这篇论文里, 欧拉将他的判别法应用到 82421, 100981, 262657, 它们是素数, 以及 1000009, 233033, 32129, 它们不是素数 (索引同上, pp.321–327); 在这里他注意到 32129 具有唯一的表示 95^2+125^2 (但不是正常表示), 而 233033 的情形, 它不是两个平方数之和, 他对其使用了一个他不曾证明过的结果, 即, 每个素数 $p=4m+1$ 都是两个平方数之和; 我们已经知道, 它只在这篇文章写成后不久才被证明的 (参看前面的 §5(b) 以及 §9).

当然, 给定一个大数 $n=4m+1$, 用反复试验的方法来寻找表示 $n=a^2+b^2$ 是不可行的; 必须设计出便捷的方法. 有两篇文章 (*Eu.*I-3,1–45=E283;1760,*Eu.*I-3,112–130=E369;1765) 致力于用上面的判别法搜寻大素数; 欧拉的想法是使用同余式. 譬如, 如果 $n\equiv 2 \pmod 3$, 那么 a 和 b 必定与 3 互素; 如果 $n\equiv 2 \pmod 5$, 则 a 与 b 必 $\equiv \pm 1 \pmod 5$; 如果 $n\equiv 5 \pmod 8$, 那么 a 和 b 必 $\equiv 2 \pmod 4$; 等等. 运用这样的附注, 欧拉便能够在许多情形把试验的总量化简到可控的大小.

特别地, 如果 $n=a^2+b^2$ 为奇数时, a 与 b 中必有一个为奇数而另一个为偶数, 故可写成 $n=a^2+4c^2$. 因此这个素性判别法完全同样地可应用于形式 X^2+4Y^2, 只要假定我们同意称一个整数 n 用形式 $\mu X^2+\nu Y^2$ 的表示 $n=\mu a^2+\nu b^2$ 为正常的当且仅当 a 与 νb 互素, 而 b 与 μa 互素就可以了. 相似地, 假定 $n=a^2+(3b)^2$, 其中 a 与 $3b$ 互素; 于是 $n\equiv 1 \pmod 3$; 如果同时我们有 $n=c^2+d^2$, 则或者 c 或者 d 必定 $\equiv 0 \pmod 3$; 由此得到这个素性判别法也适用于形式 X^2+9Y^2. 运用模 8 和模 5 的同余式, 发现以同样的方式它也可应

用于 X^2+16Y^2 以及 X^2+25Y^2, 这些观察部分地隐含在前面所引的 1765 年的文章中.

最终欧拉发现他的判别法可完全延拓到 X^2+Y^2 之外. 该判别法的主要点在于没有素数可以用两种不同的方式表成两个平方和; 这个事实依赖于作为定理 2 出现在 1747 年欧拉给哥德巴赫的信中 (*Corr.*I,416), 也作为 1749 年的论文中的命题 1 出现在 (*Eu.*I-2,302) 中, 它也再现为前面的第二章 §8 的引理 2. 当欧拉将注意力指向形式 X^2+2Y^2, X^2+3Y^2 时, 他发现形式 X^2+Y^2 的大部分理论, 包括定理和它的证明都可以轻易地拓展到那两个形式 (*Eu.*I-2,459–492=E256;1753,*Eu.*I-2,556–575=E272;1759; 参看前面的 §9, 以及第二章 §12). 特别地, 它们两者都产生了类似于上面所讨论的那种判别法; 譬如, 欧拉运用它证明了 67579 是个素数而 40081 不是 (*Eu.*I-2,490–491).

欧拉必定在某个时刻开始留意对于上面所引述的这个关键结果的证明 (第二章的 §8 的引理 2) 不仅对所有形式 X^2+NY^2 保持有效, 而且甚至对于所有形式 $\mu X^2+\nu Y^2$ 也有效, 使得特别地有, 如果 $\mu a^2+\nu b^2$ 为正, 则当它可以用两种不同的方式写成 $\mu a^2+\nu b^2$ 时它必不是素数. 1778 年, 欧拉的助手们写出了对此的若干证明或者证明概述, 同时还有对以两种不同方式分解一个写成 $\mu a^2+\nu b^2$ 的整数的一个规则 (*Eu.*I-3,422–423,*Eu.*I-4,271,*Eu.*I-4,305–310, 等等); 它们写得笨拙, 没有什么说服力. 实际上重现于第二章 §8 的欧拉 1747 年的证明可以容易地使其适用于一般的情形. 首先取 $n=\mu a^2+\nu b^2$, 假设 $q=\mu x^2+\nu y^2$ 是 n 的一个素因子, 但不除尽 $\mu\nu$. 根据欧拉熟知的一个恒等式 (参看, 譬如他的《代数学》的第 179 条:*Eu.*I-1,424), 我们有

$$nq=(\mu ax\pm\nu by)^2+\mu\nu(ay\mp bx)^2.$$

与此同时, q 除尽整数

$$ny^2-b^2q=\mu(ay-bx)(ay+bx);$$

由于它与 μ 互素, 它必除尽整数 $ay\mp bx$ 中的一个; 由于 q^2 除尽 nq, 这表明 q 除尽 $\mu ax\pm\nu by$. 写成

$$\mu ax\pm\nu by=qu,\ ay\mp bx=qv,$$

得到

$$\frac{n}{q}=u^2+\mu\nu v^2.$$

特别地, 对 $\mu>0$, $\nu>0$, $\mu\nu>1$, 这表明 $n=q$ 蕴涵了 $u=\pm1$, $v=0$; 因此没有素数可以写成 $\mu a^2+\nu b^2$ 这样的两种不同的方式, 这就是要证明的. 当然同样

的结论在今天容易用一点域 $\mathbb{Q}(\sqrt{-\mu\nu})$, 或更恰当地, 在环 $\mathbb{Z}[\sqrt{-\mu\nu}]$ 中的理想理论就能得到.

无疑上面的这个观察加之欧拉关于大素数的经验, 必定促使他去寻找使得最后提到的结果有逆的那些 μ 和 ν 的值; 这样一些值于是会产生出素性判别法, 从而推广已经知道的那些. 这相当于要求 (μ,ν) 这一对数使得每个与 $\mu\nu$ 互素的奇整数, 只要它有一个也只有一个如 $\mu a^2+\nu b^2$ 这样的表示, 并且为正常表示, 那么它就是个素数. 这个问题必定使欧拉和他的助手们忙了一阵, 直到 1778 年终于有了一个答案, 以及一个从 1 到 1848 中提出来的列表, 使得当乘积 $\mu\nu$ 是该列表中的一个整数时, 这一对 (μ,ν) 便具有了所考虑的性质; 他称这些数为 "*numeri idonei*"("合适的数", 即适合于检验大整数素性的数). 1778 年 5 月, 欧拉寄给他的朋友, 前柏林同事, 瑞士数学家 Béguelin 一份简短的关于这些发现的说明 (*Eu.*I-3,418–420=E498;1778), 后者又将它给了拉格朗日; 两个人都要求得到更多的细节. 这些由欧拉的年轻朋友, 巴塞尔的 N. Fuss 于 1778 年 6 月 30 日寄了出去 (*Eu.*I-3,420–428=E708a). Fuss 也已交给了在巴塞尔的丹尼尔 · 伯努利一份相似的报告. 丹尼尔在 1778 年 3 月 18 日有一封缺乏热情的复信, 内容如下:

"*...Ce que vous me dites tant de votre part que de celle de M. Euler est sans doute infiniment plus sublime; je veux parler du beau théorème de M.Euler sur les nombres premiers et de sa nouvelle méthode pour examiner tel nombre qu'on propose, quelque grand qu'il puisse être, s'il est premier, ou non. Ce que vous vous êtes donné la peine de me dire sur cette matière m'a paru fort subtil et digne de notre grande maître. Mais ne trouvez-vous pas que c'est presque faire trop d'honneur aux nombres premiers que d'y répandre tant de richesses, et ne doit-on aucun égard au goût raffiné de notre siècle? Je ne laisse pas de rendre justice â tout ce qui sort de votre plume et d'admirer vos grandes ressouces pour surmonter les difficultés les plus épineuses; mais cette admiration se redouble quand le sujet peut mener à des connaissances utiles. Je range dans cette classe les profondes recherches dont vous me parlez, sur la force des poutres...*" ["您告诉我您自己的和欧拉先生的东西无疑是极其令人兴奋的; 我指的是欧拉先生关于素数的美丽定理和他决定一个不管多大的数是否是素数的新方法. 您不嫌麻烦告诉我这个问题的有关方面, 在我看来似乎是非常精巧的, 与我们伟大的专家完全相匹配. 但是, 请问, 难道不是把过多的荣耀给了素数, 把如此宝贵的东西遍洒于它, 从而把不尊重他人的取向归咎到我们时代的优雅情趣吗? 我给予来自您笔下的任何东西都以适当的尊重并钦佩您克服棘手难题的强大能力, 但是当课题能走向知识的有用的部分时, 我将加倍地钦佩, 以我的观点看来, 这包括了您对梁的强度

的深刻研究······" *Corr*.II,676–677].

这对于欧拉来说根本不是新的; 他完全知道他同代人, 单单除了拉格朗日外, 对他的算术工作是多么地没有兴趣 (参看第二章 §17). 不管怎样, 在 1778 年 3 月 16 日 (几乎是伯努利写信给 Fuss 的同一天), 他有三篇关于 "*numeri idonei*" 及其应用的文章递交给了彼得堡科学院 (*Eu*.I-4,269–289=E708;*Eu*.I-4,303–328=E715; *Eu*.I-4,360–394=E719); 还有一篇加进了 4 月 20 日的文集中 (*Eu*.I-4,395–389= E725). 它们总体上整理得如此不好, 阐述和证明如此混乱和有缺陷, 以致人们很想把它们归咎于各式各样的、欧拉不能紧密掌控的助手们. 试图从这些文章里重新构造 "*numeri idonei*" 的完整理论会是一项无望的任务[6]; 对于我们的目标来说, 下面的简短叙述就足矣.

欧拉的列表由 65 个整数组成, 其中的 37 个无平方因子, 其余的由前面那些中的某个与 4, 9, 16, 25 或 36 的乘积组成; 对于后者欧拉给出了特定的规则 (*Eu*.I-4,280–288, 定理 1 到 9; 参看 F. Grube, 脚注 6,§10). 高斯在二十来年之后的《*Disquisitiones*》(第 303 条) 中顺带注意到, 欧拉的这些数正好是那些整数 N, 使得每个具有 "行列式" $b^2 - ac = -N$ 的 "正常本原" 的正形式 $aX^2 + 2bXY + cY^2$ (即 a, $2b$, c 没有公因子的这种形式) 是 "*anceps*", 这等于说, 它或者等价于一个形式 $\mu X^2 + \nu Y^2$, 其中 $\mu\nu = N$, 或者等价于形式

$$\frac{1}{2}\mu(X+Y)^2 + \frac{1}{2}\nu(X-Y)^2,$$

其中 $\mu\nu = N$ 以及 $\mu \equiv \nu \pmod 2$. 对于无平方因子的 N, 一个等价的定义是说, N 若无平方因子, 则是 "*idoneus*(合适的)" 当且仅当 $X^2 + NY^2$ 的每个与 $2N$ 互素的素因子 p 使得或是 p 自己或是 $2p$ (或两者) 可写成 $\mu a^2 + \nu b^2$, 其中 $\mu\nu = N$. 人们或许会相当怀疑是否欧拉注意到过最后的这个性质: 由于欧拉对于诸如 $\mu X^2 + \nu Y^2$ 这一类形式的广泛经验, 这个性质肯定吸引过他. 无论什么情形, 有一点是可以肯定的, 即在有意挑出 "*numeri idonei*" 来之前, 他必定已聚集了大量的数据.

我们不想对欧拉文章中的 "*numeri idonei*" 所提出的定义进行分析, 也不想对那里的所叙述的决定哪个整数是如此的判别法进行研究; 后面这个涉及仔细检查对于 $a^2 \le 3N$ 的整数 $N + a^2$ 必定基于在某个下降法之上, 或许就类似于拉格朗日的简约方法. 在欧拉的列表上的数正好是那些回应了高斯的简单定义的这个事实表明, 在这个场合, 他的直觉是健全的.

关于他的这些数, 特别使欧拉高兴的是它们让他发现了相当大的一些新素

[6] 可以在 F. Grube 严谨的文章 (*Zeitschr, für Math. u. Phys.* XIX (1874),pp.492–519) 中找到这样的理论, 与其一起的还有一篇释义性文章和对欧拉文章的详细批评; 它基于的是高斯的二次型理论. 也可参看 J.Steinig, *Elem.d.Math.* XXI (1966),pp.73–88.

数; 例如, 利用最大的那个 1848, 他能容易地建立 $18518809 = 197^2 + 18480000$ 的素性 (*Eu.*I-3,420,*Eu.*I-4,385–389). 他也试图将他的列表超出 1848, 他告诉我们, 他测试过直到超过 10000 的所有整数. 使他绝对吃惊的是, 他居然一无所获; 他现在有了一个猜想, 即这样一个自然定义的数的集合明显应该是有限的, 这对他来说是个新的体验. ("*Insigne istud paradoxon...circa nullam adhuc aliam seriem observatum esse memini*" :*Eu.*I-4,396 于 E725 中; 参看 *Eu.*I-3,420 于 E498 中). 对我们来说它的出现一点也不感到吃惊, 这是因为我们知道对于一个 "行列式" $-N$ 的 "类" 的个数随着 N 增大和要快于 N 分解为 $N = \mu\nu$ 两个因子的个数的增长. 对于 "*numeri idonei*" 个数有限的形式证明, 参看 W. E. Briggs 和 S.Chowla的文章, *Can. J. of Math.* 6 (1954), pp. 463–470. 似乎还不知道有没有超出欧拉列表的这种数.

§3.11 四平方数之和

欧拉对数论的兴趣首先是被费马关于四平方数之和的陈述唤醒的 (参看前面, §4); 但他聪明地推延了从事这项研究, 直到他在两个平方数和问题上取得了充分的进展. 从 1747 年往后, 我们发现在他的通信里越来越多地提及三个和四个平方数之和 (参看 §5(b)); 但并没有什么真正的进展, 直到他发现了 (或许是用纯粹的猜测: 参看 *Eu.*I-6,312 于 E407 中;1770) 关于四平方数和的著名恒等式: 如果

$$m = a^2 + b^2 + c^2 + d^2,\ n = p^2 + q^2 + r^2 + s^2,$$

则

$$mn = A^2 + B^2 + C^2 + D^2,$$

其中已经令

$$A = ap + bq + cr + ds, \qquad B = aq - bp - cs + dr,$$
$$C = ar + bs - cp - dq, \qquad D = as - br + cq - dp;$$

于是显然有

$$\frac{m}{n} = \left(\frac{A}{n}\right)^2 + \left(\frac{B}{n}\right)^2 + \left(\frac{C}{n}\right)^2 + \left(\frac{D}{n}\right)^2$$

(*Corr.*I,452;1748; *Eu.*I-2,368–369 于 E 242 中;1751).

接下来的一年, 在对两个平方数之和问题达到完全成功 (参看前面的 §5(b) 以及 §9) 之后, 欧拉试图将这同一种方法结合上面的这个恒等式应用到四平方和上 (*Corr.*I,495–497;1749,521;1750,527;1750, 以及 *Eu.*I-2,338–272=E242;11751); 明显地, 这要求以下两个步骤.

首先, 他必须证明每个素数除尽一个四平方数之和. 对此他证明了更多, 指出如果 p 为任一素数, 则 $x^2 + y^2 + z^2 \equiv 0 \pmod p$ 有一个非平凡解, 即一个不同于 $(0,0,0)$ 的解; 后来, 在一篇关于同一主题的决定性文章中 (*Eu.* I-3, 218–239=E445;1772), 他甚至将此拓展到一个任意的同余式 $\lambda x^2 + \mu y^2 + \nu z^2 \equiv 0 \pmod p$, 其中 λ, μ, ν 与 p 互素; 事实上, 他从实质上看出, 函数 $x \mapsto x^2 \pmod p$ 取 $(p+1)/2$ 个不同的值, 即 0 和模 p 的二次剩余; 因此同样的对于函数 $x \mapsto \lambda x^2$ 和 $x \mapsto -\mu x^2 - \nu$ 也一定成立, 故而那两个集合至少有一个公共元.

其次, 必须证明任何除尽和 $a^2 + b^2 + c^2 + d^2$ (其中 a, b, c, d 没有公因子, 但其中有些可为 0) 的素数本身也具有这样一种和. 在这里欧拉不能使他曾用于两个平方和的方法适用于此, 他所能做的全部便是证明所有的素数从而所有的整数总是四个有理数的平方和. 事实上, 假设并非如此并且设 p 是最小的不能表示成这样和的素数. 设 (a, b, c) 为 $x^2 + y^2 + z^2 \equiv 0 \pmod p$ 的一个非平凡解; 在这里我们可以假定 a, b, c 全都 ≥ 0 且 $< p/2$. 令

$$N = a^2 + b^2 + c^2 = pN',$$

故而 $N < \frac{3}{4}p^2$, $N' < p$. 由于 N' 的所有素因子均 $< p$, 故他们均是四个有理数平方和, 根据欧拉的恒等式值 N' 也是这样的和; 同样的理由知, $p = N/N'$ 因而是四个有理数的平方和. 在这个结果与费马的定理之间, 欧拉意识到仍旧有一个大缺口, 他发现自己还没有能力在其间架上桥梁 (参看附录 II).

这件事停在那里二十多年, 直到 1772 年, 他从拉格朗日那里收到费马定理被完全证明的文章 (*Lag.*III,189–201; 参看 *Eu.*IV A-5,492); 那个证明建立在欧拉关于两个平方和工作的基础上. 欧拉必定立刻重拾起了这项工作, 在 1772 年 9 月 21 日提交给彼得堡科学院, 并首次发表在 1773 年的《*Nova Acta Eruditorum*》中的一篇光辉文章 (*Eu.*I-3,218–239=E445) 里, 他首先祝贺拉格朗日的成就, 然后恰当地形容拉格朗日的证明为 "不自然的和不精细的" ("*nimis longe repetita et vehementer operosa*": 索引同上, p.218), 他则给出了对于两个平方和证明的一个新的、优美的版本 (同上,pp.222–224), 最终证明了它不仅同等地应用于形式 $X^2 \pm 2Y^2$ (同上,pp.225–226,*Eu.*I–3,275 于E449 中, 1772) 和 $X^2 + 3Y^2$ (同上,pp. 226–227), 而且也可应用于 $X^2 + Y^2 + Z^2 + T^2$ (同上, pp. 230–231). 对后面这种情形的证明如下.

设 p 为 $\sum a_i^2$ 的一个奇素因子, 其中 a_i, $i = 1, 2, 3, 4$ 为没有公因子的整数, 并且可假定为 ≥ 0 及 $< p/2$. 令 $\sum a_i^2 = pm$, 我们有 $m < p$. 如果 $m = 2$, a_i 中有两个, 譬如 a_1 和 a_2 必为奇数, 而其他的为偶数; 于是我们有

$$p = \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2,$$

从而 p 是四个平方数之和; 因此我们可设 $m > 2$. 对于每个 i, 令 $a_i = b_i + mc_i$, 其中 $|b_i| \le m/2$; 于是 $\sum b_i^2 \equiv 0 \pmod m$, 我们从而可写成 $\sum b_i^2 = mn$. 由于这些 a_i 没有公因子, 故这些 b_i 不全为 0, 且也不全都为 $\pm m/2$, 故 $0 < \sum b_i^2 < m^2$ 以及 $0 < n < m$. 现在将欧拉的恒等式应用到 $\sum a_i^2$ 和 $\sum b_i^2$ 上; 这给出了 $m^2pn = \sum A_i^2$, 其中 $A_1 = \sum a_ib_i$, A_2, A_3, A_4 由

$$A_2 = a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3 = m(c_1b_2 - c_2b_1 - c_3b_4 + c_4b_3)$$

给出, 而对 A_3 和 A_4 有两个相似的公式. 因为 m^2pn 和 A_2^2, A_3^2, A_4^2 均是 m^2 的倍数, 所以我们可以对所有的 i 令 $A_i = mB_i$, 从而得到 $pn = \sum B_i^2$. 令 d 为这些 B_i 的公因子, 并对所有的 i 写成 $B_i = da_i'$, 于是 d^2 除尽 pn. 因为 $0 < n < m < p$, d 必与 p 互素, 从而 d^2 必除尽 n; 令 $n = d^2m'$. 因此我们有 $pm' = \sum a_i'^2$; 这是一个没有公因子的四平方数之和, 并且是小于 pm 的 p 的倍数. 按此方式继续进行, 我们得到 p 自己表示成四个平方数之和, 这就是要证明的.

一个多世纪以后, 赫尔维茨 (Hurwitz) 对这同一个定理写了一个证明, 它建立在整四元数非交换环以及这个环具有欧几里得算法这个事实的基础上 (参看他的《*Math. Werke*》,II,303–330); 不知他注意到没有, 它在本质上只不过是把欧拉的证明用四元数语言重抄罢了.

§3.12 平方根与连分式

欧拉对于 "佩尔方程" $x^2 - Ny^2 = 1$ 的兴趣出现在 1730 年, 明显是由他与哥德巴赫的通信引起来的 (参看前面的 §4). 在那个时候他已经看出对于它的逐次解构成了 "由两个几何级数合成" 的 "递归" 序列 (*Corr.*I,37;1730; 参看下文的 §13); 以 $N = 8$ 的情形为例, 这意味着递次的整数 $y_0 = 0$, $y_1 = 1$, $y_2 = 6$ 等等, 它们每一个的平方是个 "三角数" (即具有形式 $\frac{1}{2}n(n+1)$, 或者 $\frac{1}{8}(x^2 - 1)$, 其中 $x = 2n + 1$), 而它们则由

$$y_n = \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{4\sqrt{2}}$$

给出 (*Corr.*I,36), 并满足递归关系

$$y_{n+1} = 6y_n - y_{n-1}$$

(*Corr.* I,30). 很快他便发表了关于该主题的一篇短文 (*Eu.*I-2,6–7=E29;1733), 主要致力于解更一般的方程 $y^2 = ax^2 + bx + c$ (参看下文 §13), 但包含了对布龙克尔解 "佩尔方程" 的方法的描述 (参看第二章 §13), 像他一直做的那样, 在那

里仍将此方法归属于佩尔和费马, 对于后者他也没有给出明显的理由; 他以处理 $x^2-31y^2=1$ 对它进行了描述 (索引同上, p.13) 并补充了一个重要的考察, 即 $p^2-Nq^2=1$ 的解给出了对于 $\sqrt{N}$ 的一个好的有理逼近 p/q (同上, p.15); 阿基米德那时就已经知道这点了 (参看第一章 §8).

至于连分式, 它们第一次出现在欧拉那里, 是在一个全然不同的背景下 (*Corr.* I,58–59;1731), 即与里卡蒂微分方程有关的地方; 但是很快他就因它们自身的原因而对其感到了兴趣 (参看 *Eu.*I-14,187–215=E71;1737), 不经意间观察到了有理数具有有限连分式表示 (由等同于欧几里得辗转相除法得到), 以及周期连分式表示了二次无理性, 并且也注意到了任一实数展成的连分式提供了对该数的最好有理逼近. 这中间的一些已为惠更斯所知 (参看前面, 第二章,§17), 但欧拉明显没有留意到惠更斯有关这方面的工作.

由于布龙克尔对佩尔方程 $x^2-Ny^2=1$ 的解和 $\sqrt{N}$ 的连分式都提供了对 $\sqrt{N}$ 好的有理逼近, 这使得欧拉想到要将他们相互进行比较. 当他这样做时 (*Eu.*I-3,73–111=E323;1759), 他发现这两个算法事实上就是同一个.

为验证这个事实, 考虑布龙克尔的方法 (欧拉总称其为 "佩尔方法 (*methodus Pelliana*)"), 这我们已在第二章的 §13 中叙述过. 它在于构造一个二次型的序列 $F_0, F_1, \cdots$,

$$F_i(X_i, Y_{i+1}) = A_iX_i^2 - 2B_iX_iX_{i+1} - C_iX_{i+1}^2,$$

并以

$$F_0(X_0, X_1) = NX_0^2 - (nX_0 + X_1)^2$$

为起始项并定义如下. 对于每个实数 ξ, 以 $[\xi]$ 表示满足 $m \leq \xi \leq m+1$ 的整数 m, 并取 $n=[\sqrt{N}]$; 然后对于每个 $i \geq 0$ 记 ξ_i 为 $F_i(\xi,1)$ 的正的根, 并且令 $m_i=[\xi_i]$, 那么我们取 F_{i+1} 为在变换 $X_i = m_iX_{i+1}+X_{i+2}$ 下 $-F_i$ 的变形. 这给出了

$$B_i^2 + A_iC_i = N,\ \xi_i = \frac{B_i+\sqrt{N}}{A_i},\ m_i = \left[\frac{B_i+n}{A_i}\right],\ C_{i+1} = A_i.$$

与此同时, 根据 F_i 的定义我们有

$$\sqrt{N} = n + \frac{1}{\xi_0},\ \xi_i = m_i + \frac{1}{\xi_{i+1}} \quad (i=0,1,2,\cdots),$$

从而 $\sqrt{N}$ 由 "连分式"

$$\sqrt{N} = n + 1/(m_0 + 1/(m_1 + 1/(m_2 + \cdots)))$$

给出.

另一方面, 在欧拉的表示中有一个递推公式 (索引同上, p. 82), 它在我们的记号下因而可以写成

$$m_i = \left[\frac{B_i + n}{A_i}\right], \qquad B_{i+1} = A_i m_i - B_i,$$

$$A_{i+1} = \frac{N - B_{i+1}^2}{A_i} = A_{i-1} + m_i(B_i - B_{i+1}),$$

且具有初始值 $B_0 = n$, $A_0 = N - n^2$; 立刻可看出它们等价于上面所给过的.

一旦布龙克尔的方法以这种方式重新解释后, 在第二章 §13 证明过的事实便有了进一步的推论. 首先它们蕴涵了 $\sqrt{N}$ 的连分式是周期的; 更准确地说, 存在一个 $p > 0$ 使得对所有的 $i \geq 0$ 有 $m_{p+i} = m_i$; 这出现在当 p 取得使 $F_0 = F_p$; 于是 $A_{p-1} = C_p = 1$. 现在像在第二章 §13 中那样, 写成 $F_i = (A_i, B_i, C_i)$, 并又一次令 $G_i = (C_i, B_i, A_i)$; 已经证明过 G_i 可以从 G_{i+1} 推导出来, 这完全像 F_{i+1} 从 F_i 推导出一样, 具有值 m_i, 这等于是说, 如果 m_i 如前, 并且 η_{i+1} 是 G_{i+1} 的正根, 我们则有

$$m_i = [\eta_{i+1}] = \left[\frac{B_{i+1} + n}{C_{i+1}}\right].$$

由于我们有 $F_p = F_0 = (N - n^2, n, 1)$, 故有

$$G_p = (1, n, N - n^2), \ \eta_p = n + \sqrt{N}, \ m_{p-1} = 2n,$$

故而 $F_{p-1}(X_{p-1}, X_p)$ 是在变换 $X_{p+1} = X_{p-1} - 2nX_p$ 下 $-F_p(X_p, X_{p+1})$ 的变形; 这给出了 $F_{p-1} = G_p$. 这表明 G_{p-1} 与 F_0 相同, 因此 G_{p-2} 与 F_1 相同, 从而由对 i 的归纳, G_{p-i} 与 F_{i-1} 相同; 由此我们得到, 对 $1 < i < p$ 有 $\eta_{p-i} = \xi_{i-1}$, $m_{p-i-1} = m_{i-1}$. 这就是所谓序列 (m_i) 的 "回文" 性质, 它意味着我们有

$$(m_0, m_1, m_2, \cdots, m_{p-2}) = (m_{p-2}, m_{p-3}, m_{p-4}, \ldots, m_0).$$

在欧拉关注于平方根 $\sqrt{N}$ 的连分式的性质以及它们在解佩尔方程的使用时, 没有迹象表明他曾寻求除了实验根据以外的任何东西来支持他的发现. 他确实提到过在他的过程中对于整数 B_i, A_i, m_i 必须有界 (对所有 i 有 $B_i \leq n$, $A_i \leq B_i + n$, $m_i = 2n$ 或 $m_i \leq n$: 索引同上 p.83); 由此则可以至少推出结论说, 序列 (m_i) 从某一项开始是周期的, 但是他没有提到这一点, 或者不屑于去提.

很久以后他又回到了这个课题 (*Eu*.I-3,310–334=E454;1772), 把他的观察扩展到了其他二次无理性连分式, 特别是对于平方根 $\sqrt{r}$, 其中 r 是任意大于 1 的有理数; 对于后者事实上可以完全像上面那样, 证明其连分式的周期性和回文特性, 这时我们将

$$F_0(X_0, X_1) = bX_0^2 - a(nX_0 + X_1)^2$$

作为序列 (F_i) 的起始点, 其中已经置 $r = b/a$ 以及 $n = [\sqrt{r}]$. 在这同一篇文章里, 欧拉也将连分式用于确定 $|F(a,b)|$ 在 a, b 取非 0 整数时的极小值上, 这里的 F 是个任意的不定二元二次型.

这一次他就来得太迟了. 1768 年, 第一次着手数论, 并且还多少有些笨拙的拉格朗日证明了关于佩尔方程的所有基本定理 (*Lag.*I,671–731); 没有多久, 他给出了被认为是这个课题的一个决定性的处理, 其基础是连分式算法 (*Lag.*II,494–496); 它在本质上就是我们在第二章 §13 中所叙述的; 它包含在一篇 1769 年在柏林发表的长论文中 (*Lag.*II,337–535;1768); 1769 年或 1770 年初到了欧拉手中 (参看 *Eu.*IV A-5,466), 与其一起的还有许多其他的贡献, 欧拉对它们必定给予了更多的关注. 拉格朗日的解连同对这同一主题的其他更多的结果被他放到他对欧拉的《代数学》的 "附件" (写于 1771 年但仅在 1773 年才出版; 参看下文的第四章 §2) 中了; 在那里他也给了与欧拉在他的文章 E454 中讨论过的同一个二次型的极小值问题的一个详细的处理. 这也没有得到欧拉的重视 (参看第四章 §3 , 以及前面的 §9). 在他后来当欧拉重回佩尔方程这个课题时 (*Eu.*I-4,76–90=E559;1773), 他对那时已成为关于这个课题的普通知识再也没有任何实质性的补充了.

§3.13 二次丢番图方程

在 1730 年, 在他关于 "佩尔方程" 的所有后续工作中 (参看前面的 §12), 欧拉已习惯于在一个二元二次丢番图方程的更加广阔的架构中讨论那些课题, 这些方程或者要求整数解, 或者像丢番图那样要求有理数解. 许多年里他都局限于丢番图研究过的类型 $y^2 = \alpha x^2 + \beta x + \gamma$ (参看第一章 §10) 上. 在 1759 年 (或者也许是 1763 年, 因为手稿似乎曾经修改过) 他简短表示他也将他考察的范围拓展到了更一般的类型

$$F(x,y) = Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$$

(*Eu.*I-3,76 于 E323 中;1759); 但而后这个课题停下了, 直到 1772 年, 那时在一篇文章中该方程由于本身的原因又被拾起 (*Eu.*I-3,297–309=E452;1772), 或许是想作为对拉格朗日关于这同一主题工作的补充吧 (参看第四章 §2).

或许除了也是在 1772 年的一个场合外 (参看前面的 §9), 欧拉总是解释说, 除非事先至少知道了一个解, 不管是怎样知道的 (大体是 "猜测" 的, "*quasi divinando*": *Eu.*I-2,610), 否则他什么也做不了. 在牛顿都已知道的几何解释 (参看前面的第二章,§15) 中, 有理地解一个二次方程 $F(x,y) = 0$ 的一个方法是, 一旦给出了一个解 (a,b), 则以任意一条通过 (a,b) 的直线去交二次曲线 $F = 0$; 我

们在 (第一章 §10) 已经看到了, 而这可追溯到丢番图. 欧拉并没有提及这个解释, 但当他用代数语言叙述那个方法时, 它可能完全隐藏在他的思想的背后; 他的代数方法首先出现在 1758 年对 $y^2=\alpha x^2+\beta x+\gamma$ 的处理上, 然后是 1772 年对一般情形. 取 (a,b) 为一个解, 然后用直线

$$\frac{x-a}{p}=\frac{y-b}{q}$$

去交曲线 $F=0$ (*Eu.*I-2,578 于 E279 中;1758; *Eu.*I-3,299 于 E452 中;1772), 他得到了由下面公式给出的交点 (a',b'):

$$a'=\lambda a+\mu b+\sigma,$$
$$b'=\nu a+\rho b+\tau,$$

其中这些系数是 p 和 q 的有理函数. 用现代语言说, 容易验证由

$$(x,y)\mapsto(\lambda x+\mu y+\sigma,\nu x+\rho y+\tau)$$

线性变换

$$S=\begin{pmatrix}\lambda\ \mu\ \sigma\\ \nu\ \rho\ \tau\end{pmatrix}$$

将 F 变到自己; 因此它的齐次部分

$$S_0=\begin{pmatrix}\lambda\ \mu\\ \nu\ \rho\end{pmatrix},$$

即变换

$$(X,Y)\mapsto(\lambda X+\mu Y,\nu X+\rho Y)$$

将 F 的齐次部分

$$F_0(X,Y)=Y^2-\alpha X^2,\ \text{分别地},\quad F_0=AX^2+2BXY+CY^2$$

变到自己. 换句话说, 欧拉的公式决定了形式 F_0 的自同构.

欧拉知道, 如果问题在于得到 $F=0$ 的所有有理解, 则无需对以上公式补充任何东西; 但要求整数解则是另一回事. 对此, 他的方法 (已在 1773 年写出: *Eu.*I-2,7 于 E29 中;1733; 参看 *Corr.*I,36;1730) 可描述为要构造一个具整系数的线性变换 Σ, 将 F 变到自己; 如果可以做到这点, 则将 Σ 反复地用到一个整数解上, 或许可以期待产生, 如果不是全部的话也至少是无穷多个这样的解, 当然要假定 Σ 不是有限阶的. 顺便说一下, 以上定义的变换 S 不能用到此, 这是因为它

的阶为 2; 对这种情况的失察 (这个失察可归咎于欧拉的助手们而非他自己, 这是因为他在 1758 年并没有犯此错误; 参看 *Eu*.I-2,582, 推论 2 于 E279 中;1758) 损害了他 1772 年文章的第一部分 (*Eu*.I-3,301–303).

用现代语言说, 如果 Σ 如欧拉所要求的, 那么它的齐次部分 Σ_0 必定属于 F_0 的自同构群 Γ_0, 即整系数的、且行列式 $\lambda\rho-\mu\nu=1$ 的变换, 它将 F_0 变为自己; 给定这样一个 Σ_0, 有一个唯一的 Σ (不必具有整系数) 将 F 变到自己. 像欧拉那样, 我们实质上排除掉平凡的情形, 即 F_0 的 "行列式" $\Delta=B^2-AC=0$ 的情形, 这时二次曲线 $F=0$ 是条抛物线. 于是 Σ 由 Σ_0 通过调整 σ, τ 推出 Σ, 以使 Σ 保持二次曲线 $F=0$ 的中心不变.

先举方程 $y^2=\alpha x^2+\beta x+\gamma$ 的情形; 我们像欧拉那样不仅假定 α 非零而且假定其 >0 并且不是平方数, 这是因为否则的话, 该问题就只会有有限个解, 可以用反复试验来解决它. 于是欧拉的计算 (*Eu*.I-2,8–9 于 E29 中;1733) 表明 $F_0=Y^2-\alpha X^2$ 的自同构群 Γ_0 由变换

$$\Sigma_0=\begin{pmatrix} p & q \\ \alpha q & p \end{pmatrix}$$

组成, 其中 (p,q) 是 "佩尔方程" $p^2-\alpha q^2=1$ 的任意一个解, 就像我们看到的那样 (*Eu*.I-2,600–601 于 E279;1758), 这个事实与 "婆罗摩笈多恒等式" 紧密相关, 他很可能是第一次正好在这种背景下注意到它的 (参看前面的 §8).

让 Σ_0 如上所示, 于是相应的变换 Σ 由

$$\Sigma=\begin{pmatrix} p & q & (p-1)\beta/2\alpha \\ \alpha q & p & \beta q/2 \end{pmatrix};$$

进行迭代, 它给出了

$$\Sigma^2=\begin{pmatrix} p^2+\alpha q^2 & 2pq & \beta q^2 \\ 2\alpha pq & p^2+\alpha q^2 & \beta pq \end{pmatrix},$$

它具有整系数. 因此或使用由 Σ 生成的群, 或这至少是 Σ^2 生成的群, 我们总可以从一个整数解得到无穷多个其他的整数解. 拉格朗日后来证明了, 从实质上说, 所有的解都可以由有限多个解导出 (*Lag*.II,512–522,704–705); 欧拉从没有提出过这个问题. 引起他对此兴趣的是另外的东西: 将诸如 Σ 这样的变换及其迭代 Σ^n 应用到一个给定的解 (a_0,b_0) 所生成的序列 (a_n,b_n) 具有什么性质? 他相当早就已发现的对它的答案 (*Eu*.I-2,10 于E29 中;1733; 参看 *Corr*.I.30,36;1730) 是说 (a_n), (b_n) 两个序列都是 "递归序列".

这个概念被丹尼尔在某种程度上仔细研究过, 这是在 1728 年或 1729 年的一篇文章中的 (发表在 1732 年: *D.Bern*.II,49–64), 它跟随在 A.de Moivre (棣莫

弗) 和包括丹尼尔的表弟尼古拉斯 · 伯努利和哥德巴赫在内的其他人的关于这同一主题的工作之后 (参看同上, p.49). 欧拉当然从丹尼尔写时就已熟悉了这篇文章; 他在他 1748 年的《无穷分析导论》的第 4, 13 和 17 章中熟练而全面地阐述了这个课题 (*Eu*.I-8). 称一个无穷序列 $(A_0, A_1, A_2, \cdots)$ 为 "递归的" 是说它对于所有 $n \geq 0$ 满足线性关系

$$A_{n+m} = L(A_{n+m-1}, A_{n+m-2}, \cdots, A_n);$$

这等价于说, 它的 "母级数" $\sum_0^\infty A_n x^n$ 是有理函数 $P(x)/Q(x)$ 在 $x = 0$ 的展开式, 其中 $Q(x) = 1 - L(x, x^2, \cdots, x^m)$, $P(x)$ 是一个次数 $< m$ 的多项式; 如果 L 不是齐次的而是含有常数项, 则这个陈述必须稍作改动. 特别地, 如果 Q 没有重根而是单根 $\xi_1, \xi_2, \cdots, \xi_n$, 则可写为

$$\frac{P(x)}{Q(x)} = \sum_1^m \frac{\lambda_\mu}{1 - \xi_\mu x},$$

从而

$$A_n = \sum_1^m \lambda_\mu \xi_\mu^n,$$

故而, 用欧拉的话说, 即序列 (A_n) 是 "由 m 个几何级数合成" (参看前面的 §12).

现在返回方程 $y^2 = \alpha x^2 + \beta x + \gamma$; 首先如欧拉所做 (*Eu*.I-2,589–590 于 E279 中;1758), 考虑情形 $\beta = 0$. 由给出的一个解 (a_0, b_0) 推导出的解 (a_n, b_n) 是将上面定义的变换 Σ_0 的迭代 Σ_0^n 应用于它得到的. 这对 $n \geq 0$ 给出了

$$a_{n+1} = pa_n + qb_n, \qquad b_{n+1} = \alpha q a_n + pb_n,$$
$$a_{n+2} = pa_{n+1} + qb_{n+1}, \qquad b_{n+2} = \alpha q a_{n+1} + pb_{n+1},$$

因而由于 $p^2 - \alpha q^2 = 1$, 故

$$a^{n+2} = 2pa_{n+1} - a_n, \qquad b_{n+2} = 2pb_{n+1} - b_n.$$

由递归序列的理论 ("*ex doctrina serierum recurrentium*": 同上, p.584) 知, 它们现在可写成如下形式:

$$a_n = (r + s\sqrt{\alpha})(p + q\sqrt{\alpha})^n + (r - s\sqrt{\alpha})(p - q\sqrt{\alpha})^n,$$

其中 r 和 s 是两个适当的有理数; 对于 b_n 也有相似的公式. 对于 $\beta \neq 0$, 可得到一个相应的结果 (同上, pp.584–585).

对次数 2 的方程 $F(x,y)=0$ 的一般情形, 欧拉假定 F_0 的 "行列式" $\Delta=B^2-AC>0$ 并且不是个平方数; 否则, 像他很可能知道的那样, 这个问题只有有限个解. 那么在前面的记号下, 表明原来形式 F_0 具有自同构

$$\Sigma_0=\begin{pmatrix}p+Bq & Cq\\ -Aq & p-Bq\end{pmatrix},$$

其中 (p,q) 是 $p^2-\Delta q^2=1$ 的解; 它再次可以扩充为 F 自身的一个同构 Σ (*Eu.*I-3,76 于 E323 中;1759; *Eu.*I-3,306 于 E452 中;1772), 其中 Σ 的系数 σ, τ 作为分母为 Δ 的分式出现, 而不必是整数. 欧拉知道在这种情形下 Σ^2 的系数也是整数吗? 没有提到. 另一方面, 他最终证明了在 Σ 的逐次迭代下 (a_0,b_0) 的像 (a_n,b_n) 可有以下类型的公式表达:

$$a_n=(r+s\sqrt{\Delta})(p+q\sqrt{\Delta})^n+(r-s\sqrt{\Delta})(p-q\sqrt{\Delta})^n-2r+a_0.$$

这一次, 由于最新获得的技术 (参看下文, §14), 这个证明并没有诉求于 "递归级数理论" (*Eu.*I-3,306–309 于 E452 中; 1772).

§3.14　再论丢番图方程

费马已经将二次型的理论用到了丢番图问题上 (参看第二章 §12). 当大约在 1748 年, 欧拉开始从事对费马的观察资料的研究时肯定存在同样的想法 (参看前面的 §4). 它的第一个例子是在一篇文章中给出的 (*Eu.*I-2,223–240=E167;1748; 参看前面的 §4), 那里他利用了关于形式 X^2-2Y^2 结果 (在那时还远不能证明它) 以便处理一个费马提出的丢番图问题. 与此同时, 他的注意力被费马叙述的关于 $x^n+y^n=z^n$ 的陈述所吸引 (*Corr.* I,445;1848); 1753 年他已经能够对哥德巴赫宣称他解决了 $n=3$ 的情形 (*Corr.*I,618). 就像他一些年后表示的 (*Eu.*I-2, 557 于 E272;1759), 它基于了形式 X^2+3Y^2 的理论; 那时他还没有完成它, 但已取得了决定性进展 (参看 *Eu.*I-2,481–482;*Scholion*, 于 E256 中;1753, 以及前面的 §9). 无疑, 他对于费马问题的 $n=3$ 情形的证明本质上就是我们在第二章 §16 已经叙述过的那个. 在 1754 年, 他再一次地应用这同一形式的理论于方程 $x^3+y^3+z^3=t^3$ (*Eu.*I-2,428–458=E255;1754; 也可参看 *Eu.*I-2,557); 那里的主要结果翻译成现代的话说就是, 该方程在射影空间定义的是个有理曲面; 依我们的观点看它属于代数几何.

他对于 $x^3+y^3=z^3$ 的 1753 年的证明从来就未发表过; 然而那时他曾决定把它放到他的《代数学》的最后一节中去 (参看前面 §5(c)), 在那里他为处理二次无理性设计出一个新的技术并在二元二次型理论中使用它们. 相似的思想, 甚

至更为深远的想法出现在拉格朗日关于他的代数工作中 (参看 *Lag.*II,522–535). 这是欧拉写信给拉格朗日谈关于如何发现这个巧合:

"J'ai aussi fort admiré votre méthode d'employer les nombres irrationels et même les imaginaires dans cette espèce d'analyse, qui est uniquement attachée aux nombres rationels. Il y a dejà quelques années que j'ai eu de semblables idées;...ayant publié ici une Algebre complette en langue russe, j'y ai developpé cette matiére fort au long,où j'ai fait voir que, pour résoudre l'equation

$$xx + nyy = (pp + nqq)^{\lambda},$$

on n'a qu'à résoudre celle-ci

$$x + y\sqrt{-n} = (p + q\sqrt{-n})^{\lambda}.$$

Cet ouvrage s'imprime actuellement aussi en allemand...Mais je n'y ai pas poussé mes recherches au delà des racines quarrées; et l'application aux racines cubiques et ultérieures vous a été réservée uniquement. C'est de là que j'ai tiré cette formule très remarquable

$$x^3 + ny^3 + nnz^3 - 3nxyz$$

dont les trois facteurs sont $x + y\sqrt[3]{n} + z\sqrt[3]{n^2}$*; d'où l'on voit qu'on peut toujours aisément déterminer les lettres* x, y *et* z *pour que cette formule devienne un quarré,ou un cube...ou quelque plus haute puissance"* ["我极为羡慕您在这样一种只处理有理数的分析中使用无理的甚至虚数的方法. 多年来我已经有了这种类似的想法; …… 在这里已发表了一本用俄文写的完整的《代数学》, 我已相当详尽地将它阐明, 证明了为了解

$$x^2 + ny^2 = (p^2 + nq^2)^{\lambda},$$

只要解

$$x + y\sqrt{-n} = (p + q\sqrt{-n})^{\lambda}$$

就够了. 一本它的德文译本即将出版…… 但我不会超过平方根的范围; 至于对三次和更高次根那只是您的事. 它是我所发现的令人瞩目的公式

$$x^3 + ny^3 + n^2z^3 - 3nxyz,$$

它的因子是 $x+y\sqrt[3]{n}+z\sqrt[3]{n^2}$; 由此可以看到 x, y, z 总可以容易决定以使得该公式等于一个平方的, 立方的, ……, 或更高次的幂":*Eu.*IV A-5,467;1770; 参看他的《代数学》的第 191 条, *Eu.* I-1,431]. 相似地, 在 1772 年评述这同一篇文章时, 他

写道: “*Haec methodus...eo magis est notatu digna, quod ex doctrina irrationalium eat petita, cuius alioquin nullus videtur esse usus in Analysi Diophantea. Eximium autem huius doctrinae usum iam pridem in Algebra mea Ruthenice et Germanice edita fusius ostendi*” [“这个方法由于来自无理数的理论, 看起来似乎对于丢番图分析没有什么用, 所以它更加引人注目. 然而就像我在不久前用俄文和德文出版的《代数学》中详尽表明的那样, 它是如此有用, 也是一个杰出的方法”: *Eu.*I-3,309 于 E452 中;1772].

就欧拉所关切的而言, 新的方法在于将一个二次型 x^2+ny^2 分解为因子 $x\pm y\sqrt{-n}$ 或者一个二次型 ax^2+cy^2 分解为因子 $x\sqrt{a}\pm y\sqrt{-c}$. 只要这样做仅为了推导出代数恒等式, 这个方法的使用就是无懈可击的. 当他被用于证明 “婆罗摩笈多恒等式 (Brahmagupta's identity)” 时,便是这种情形 (《代数学》的第 176 条,*Eu.*I-1,422; 参看第一章 §8) 或者更一般的恒等式

$$(ap^2+cq^2)(r^2+acs^2)=a(pr\pm cqs)^2+c(qr\mp aps)^2$$

也是如此 (同上, 第 178 条, p.424). 以同样的方式, 令

$$x\sqrt{a}\pm y\sqrt{-c}=(p\sqrt{a}\pm q\sqrt{-c})^3$$

(同上, 第 188 条, p.429), 欧拉对于

$$x=ap^3-3cpq^2,\qquad y=3ap^2q-cq^3,$$

正确地作出结论说, 数 ax^2+cq^2 成为一个立方数, 即 $(ap^2+cq^2)^3$.

然而有了这些恒等式之后要做的, 以及他在处理方程 $x^3+y^3=z^3$ 时所需要的东西 (参看同上的第 247 条, pp.492,493) 是逆问题, 一个他毫不犹豫能说清楚的逆问题. 按他所说, 如果形式 aX^2+cY^2 不能分解为有理线性因子 (即如果 $-ac$ 不是平方数), 并且当 x 与 y 互素时, ax^2+cy^2 是一个立方数, 则必有两个整数 p,q 使得 x 和 y 由上面的公式给出, 这是 “因为 $x\sqrt{a}+y\sqrt{-c}$ 和 $x\sqrt{a}-y\sqrt{-c}$ 没有公因子, 故而必为立方数” (同上第 191 条, p.431). 譬如, 如果 x^2+3y^2 是个立方数而 x 与 y 互素, 则有整数 p,q 使得

$$x=p^3-9pq^2,\qquad y=3p^2q-3q^3$$

(同上, 第 189 条, p.430).

最后的这个断言是正确的; 它只不过是我们第二章 §12, 引理 5 的内容; 它必定也已为费马所知 (参看第二章 §12 和 §16) 并且至少隐含在欧拉的关于形式 X^2+3Y^2 的理论之中, 而该理论包含在专门用来为欧拉较早时处理方程 $x^3+y^3=$

z^3 打基础的文章 E272;1759(*Eu*.I-2,556–575)里; 事实上, 所提到的这个结果就是为此目的所要的全部东西. 在他用他的新"方法"来证明它的正当性时, 他的本能没有全面误导他, 这要归功于 $\mathbb{Q}(\sqrt{-3})$ 具有欧几里得辗转相除法的事实 (参看第二章, 附录 I), 故而通常的算术定律对那个域中的整数保持了有效性. 就此方面而言, 它也使高斯做了正确的事.

但是发生了一个突然的事件. 代数数进入了数论 —— 从后门进来的.

§3.15 椭圆积分和加法定理

欧拉从两个十分不同的方面对我们现在称做的"椭圆曲线" (即亏格 1 的代数曲线) 进行了考虑, 他从不曾表示留意过它们之间的联系更没有注意到它们实质上恒同.

一方面, 无疑, 从职业生涯一开始他必定就已熟悉了处理亏格 1 的丢番图方程的传统方法 (参看第一章 §10, 第二章 §15, 以及前面的 §5(d)). 与这些方程相关联地, 他也终于想起用下降法重新构造费马的证明 (参看第二章 §16, 以及前面的 §5(d) 和 §14). 最后, 在生命后期, 他更加系统地研究了这些问题, 包括"二重方程", 这正是丢番图和费马两人的宠爱, 另外还有对 x 为二次, 对 y 也为二次的方程 $\Phi(x,y)=0$, 这也许是他对整个这个课题最具原创性的贡献了.

另一方面, 他从他的先行者那里, 特别从约翰 · 伯努利那里继承的, 对于我们称之为的"椭圆积分"的强烈兴趣, 之所以有这个名字是因为椭圆的弧长依赖于这种类型的积分; 按照难度的顺序人们认为它们与有理函数的积分邻近. 后者总可以通过对数和反三角函数表达出来, 当然是指它们的有理函数表达式, 这一点在十七世纪、十八世纪被逐渐地认识到, 直到作为确定的事实被接受 (参看 *Corr*.I,50–57 以及 170–171); 欧拉最终从所谓的"代数基本定理"将它推导了出来 (*Eu*.I-17,70–194=E163,163;1748; 参看前面的 §7). 有理地依赖于 x 和平方根 $\sqrt{ax^2+bx+c}$ 的函数于是可以用"丢番图方法"被积分出来, 即用了变量替换

$$t=\sqrt{ax^2+bx+c}-x\sqrt{a},\quad x=\frac{t^2-c}{b-2t\sqrt{a}},$$

这是与用来解丢番图方程 $y^2=ax^2+bx+c$, 其中 a 为平方数的有理解时所用的相同的替换 (参看 *Corr*.II,190 以及 *J.Bern*,III,393). 因此, 当还是青年的欧拉试图 (当然无功而返) "积出" 微分 $dx/\sqrt{1-x^4}$ (*Corr*.I,147;1730) 时, 他必定注意到这几乎是与求 $y^2=1-x^4$ 的有理解是同一个问题, 或者 (是相同的) 与求 $Z^2=X^4-Y^4$ 的整数解一样; 因此当他重新构造费马对后一方程的不可解性的证明 (*Eu*.I-2,38–58=E98;1738) 时, 这必定有助于说服他, 他所考虑的微分用已

知的函数是不可能积出来的. 事实上在这同一年, 当他给他年老的老师约翰 · 伯努利寄去他对这种类型积分的最新发现时, 他表达自己的看法如下:

"*Observavi nuper insignem elasticae rectangulae proprietatem, in qua si abscissa ponatur x, est applicata* = $\int \frac{xxdx}{\sqrt{a^4-x^4}}$ *et longitudo curvae*= $\int \frac{aadx}{\sqrt{a^4-x^4}}$ *quae expressiones ita sunt comparatae, ut inter se comparari nequeant. At si abscissa sumatur = a, inveni rectangulum sub applicata et arcu comprehensum aequale esse areae circuli cuius diameter sit abscissa=a; quae observatio mihi quidem notatu maxime digna videtur*" ["我新近发现了弹性曲线的一个引人注目的性质, 该曲线由方程 $y = f(x)$ 给出, 其中

$$f(x) = \int_0^x \frac{x^2dx}{\sqrt{a^4 - x^4}};$$

它的从 0 到 (x, y) 的弧长是

$$s(x) = \int_0^x \frac{a^2dx}{\sqrt{a^4 - x^4}};$$

这两个不定积分相互无关, 但我发现了 $f(a)s(a) = \frac{1}{4}\pi a^2$, 它对我来说似乎是最值得注意的":*Bibl.Math.*(III)5(1904),vp.291;1738; 参看 *Eu.*I-14,268 于 122 中;1739, 以及欧拉给克莱罗的信, *Eu.*IV A-5,114;1742]. 那个发现不过是把在第一类和第二类椭圆积分的周期之间的勒让德关系特别用在双纽线情形的结果.

至于欧拉后来关于椭圆积分的发现, 其故事已广为人知 (参看, 譬如 A.Enneper,《*Elliptische Functionen, Theorie und Geschichte*》,Halle 1876, 以及 *Eu.*I-20,pp.VII-VIII). 在这里我们将处理与我们的主旨最切题的方面. 适当的背景资料可参看下文的附录 III.

欧拉紧跟着同时代人对于那些积分方面的工作, 其中特别包括麦克劳林 (Maclaurin) 和达朗贝尔 (譬如参看他给达朗贝尔的信, *Eu.*IV A-5,252;1746). 1751 年 12 月 23 日, 法尼亚诺两卷本的《*Produzioni Matematiche*》刚刚出版就送到了柏林科学院并交给了欧拉; 第二卷中包含了关于椭圆积分的复印片段 (*Fag.*II,287–318), 它出现在 1714 年到 1720 年间的一份模糊不清的意大利的杂志上, 该杂志仍完全不为人知. 欧拉在读了没有几页时便立即热情澎湃; 1752 年 1 月 27 日他递交给科学院一份学术报告 (*Eu.* I-20,80–107=E252), 阐述了法尼亚诺的主要结果, 而他也已经加上了一些自己的东西.

法尼亚诺结果中最令人印象深刻的莫过于关于 "双纽线微分"

$$\omega(z) = \frac{dz}{\sqrt{1 - z^4}}$$

的变换了; 他是如何取得它们的, 即便欧拉也只能猜测了. 欧拉在 1753 年写道, "只要他的方法提供了进一步从事这些研究的确切方法, 那么他的发现肯定会使得超越函数的理论更加清晰地展示出来; 但它停留在一个带有试探性的替换上, 几乎是偶然地应用于······" ["*Hinc certe theoriae quantitatium transcendentium insigne lumen accenderetur, si modo via, qua Fagnanus est usus, certam methodum suppeditaret in huiusmodi investigationibus ulterius progrediendi; sed...tota substitutionibus precario factis et quasi casu fortuito adhibitis nititur...*":*Eu.*I-20,110 于 E263;1753).

但是他在这一年以前曾写道: "对于这个目标 [分析的进展], 这样的观察特别有价值, 而它几乎是偶然间做出来的, 是凭经验的发现, 感受到的是没有推理性的解释, 没有取得它们的直接方法······我在法尼亚诺伯爵新近出版的书里发现的是这一类的几个观察资料······" ["*Ad hunc scopum imprimis accomodatae videntur eiusmodi observationes, quae cum quasi casu sint factae et a posteriori detectae, ratio ad easdem a priori ac per viam directam perveniendi...neutiquam est perspecta...Huiusmodi autem observationes...nonnullas deprehendi in opere Ill. Comitis Fagnani nuper in luce edito*": *Eu.*I-20,81 于 E252 中;1752].

欧拉以其慷慨大度的特点从未否认过曾从法尼亚诺那里受益 (譬如参看他给 Heinsius 的信,*PkU.*109;1764); 但是的确除了欧拉没有别人能够在法尼亚诺的孤立结果中看到一个分析新分支的萌芽. 他的第一个贡献是将法尼亚诺的对于双纽线的倍量公式推广到一个一般的乘法公式 (*Eu.*I-20,100 于 252 中;1752). 像他所说, 如果本质上 $z \mapsto u = f(z)$ 将微分 $\omega(z)$ 变换到 $\omega(u) = n\omega(z)$, 那么变换

$$\text{(A)} \qquad z \mapsto v = \frac{z\sqrt{\dfrac{1-uu}{1+uu}} + u\sqrt{\dfrac{1-zz}{1+zz}}}{1 - uz\sqrt{\dfrac{(1-uu)(1-zz)}{(1+uu)(1+zz)}}}$$

便将 $\omega(z)$ 变到 $\omega(v) = (n+1)\omega(z)$. 他很快就将此重写为等价的形式

$$\text{(A}'\text{)} \qquad v = \frac{z\sqrt{1-u^4} + u\sqrt{1-z^4}}{1 + uuzz}$$

(*Eu.*I-20,65–66 于 E251 中;1753) 并且认识到它蕴涵了

$$\omega(v) = \omega(z) + \omega(u),$$

其中 z, u 被当作独立变量, 故而它完全就是双纽线积分 $\int \omega(z)$ 的加法公式.

在他的关于这个课题的第二篇文章里, 我们已经感到了他清晰地表达出了他后来发展椭圆积分的主要思想. 当然他也探测到了一些死胡同; 就这些而言,

我们会叙述他的不懈的努力，并用圆锥截线和其他曲线的弧长来对他的结果做出几何的解释 (譬如参看 *Corr.*I,568–569;1752,E264;1755, E639;1776); 还包括他精心进行的计算，以在这些计算中寻求 "一个更短且更自然的方法" ("*ein kürzerer und natürlicherer Weg*":*PkU.* 109;1764; 参看 *Eu.*I-20,305–311 于 E345 中;1765) 从而证明在加法定理中本质性的东西. 对于后面的这个尝试他有如下的评述: "我不能否认它做起来会如此迂回曲折，以致人们不能期待那些运算能同时出现在任何单个人的思想里" [*Diffiteri non possum, hoc per multas ambages esse praestitum, ita ut vix expectandum cuiquam has operationes in mentem venire potuisse*":*Eu.*I-20,311].

对欧拉首要的冲击似乎是法尼亚诺的工作给他提供了一个微分方程 $\omega(x) = \omega(y)$ 的代数积分 (除平凡的 $x = y$ 外), 这由 $x^2y^2 + x^2 + y^2 - 1 = 0$ 给出. 很快他必定已注意到他的公式 (A), 或者等价的 (A′), 隐含着同一方程的通积分; 在 (A′) 中用 y, x 和一个常数 c 分别置换 v, z 和 u 后, x 和 y 之间的关系是可以写为

$$\text{(B)} \qquad c^2x^2y^2 + x^2 + y^2 = c^2 + 2xy\sqrt{1-c^4}$$

(*Corr.*I,567;1752;*Eu.*I-20,63 于 E251 中;1753), 对于 $c = 1$ 它化成了法尼亚诺的方程.

或许法尼亚诺有点受到了与方程

$$\frac{dx}{\sqrt{1-x^2}} = \frac{dy}{\sqrt{1-y^2}}$$

类比的引导吧. 无论如何, 欧拉用起它来感到十分自在和系统, 并看出最后面的那个方程有一个通积分 (他情愿称其为 "完全" 积分):

$$x^2 + y^2 = c^2 + 2xy\sqrt{1-c^2}$$

(*Corr.*I,567;1752); 这当然是令方程的两端都等于 dt, 然后取 $x = \sin t$, $y = \sin(t + t_0)$, $c = \sin t_0$ 得到的. 他马上就看出, 对于 $\omega(x)$, $\omega(y)$ 的类似处理 "是不可能的或者至少不是现成可用的" ["*huiusmodi comparatio in formulis transcendentibus* $\int dx/\sqrt{1-x^4}$ *et* $\int dy/\sqrt{1-y^4}$ *locum non habet seu saltem non constat*":*Eu.* I-20,61]. 如果他深入追寻这个思想, 他就会, 如我们现在可以知道的那样, 发现雅可比椭圆函数, 或者至少像高斯所做的那样, 发现 "双纽线" 正弦和余弦. 然而取而代之的是, 在使用 "不是确知的方法而是臆想的手段" ["*nulla certa methodo...sed...tentando vel divinando*" 同上,p.61] 得到所希望的积分后, 他仅仅按经验用取微分的方法验证了 (B) 并同时应用它以 y 来表达 x, 以 x 来表达 y.

自此以后, 欧拉处理椭圆积分总是停留在对 x 的次数 ≤ 2, 对 y 的次数也 ≤ 2 的关系式 $\Psi(x,y)=0$ 上. 这样一个关系可写成

$$\Phi(x,y)=P_0(x)y^2+2P_1(x)y+P_2(x)=0$$

或者也可写成

$$\Phi(x,y)=Q_0(y)x^2+2Q_1(y)x+Q_2(y)=0,$$

其中 P_i, Q_i 都是次数 ≤ 2 的多项式. 或者解出 y 或者解出 x, 我们便看出由 $\Phi=0$ 定义的曲线双有理等价于两条曲线 $z^2=F(x)$ 和 $w^2=G(y)$ 中的任一条, 其中

$$F=P_1^2-P_0P_2, \qquad G=Q_1^2-Q_0Q_2.$$

因此关系式 $\Phi=0$ 可以用来建立两条曲线 $z^2=F(x)$, $w^2=G(y)$ 之间的同构; 欧拉偶尔用过这个想法 (参看 *Eu*.I–20,69–71,77,248–249).

另外, 我们在这里有

$$\frac{1}{2}\frac{\partial\Phi}{\partial x}=Q_0(y)x+Q_1(y)=\pm\sqrt{G(y)},$$

$$\frac{1}{2}\frac{\partial\Phi}{\partial y}=P_0(x)y+P_1(x)=\pm\sqrt{F(x)},$$

故而对关系式 $\Phi=0$ 取微分, 得到

$$\pm\frac{dx}{\sqrt{F(x)}}=\pm\frac{dy}{\sqrt{G(y)}}$$

(这是 F 与 G 具次数 3 或 4 时的 "一般情形" 中曲线 $\Phi=0$ 上的第一类微分). 我们也可以说, 如果适当地选取符号, 上面定义的两条曲线 $z^2=F(x)$, $w^2=G(y)$ 之间的同构则将微分 dx/z 和 dy/w 相互变换.

欧拉几乎永远不变地将自己限制于 Φ 对 x 和 y 对称的情形; 于是他将它写成

$$\alpha+2\beta(x+y)+\gamma(x^2+y^2)+2\delta xy+2\varepsilon xy(x+y)+\zeta x^2y^2=0$$

并称其为 "典则方程 (Canonical equation)" (*Eu*.I-20,321 于 E347 中;1765; 参看 *Eu*.I-20,71 于 E251 中;1753 以及 *Eu*.I-20,155 于 E261 中;1755). 这里的 F 和 G 是同一个多项式并且用欧拉的话说 $\Phi=0$ 是微分方程

$$\pm\frac{dx}{\sqrt{F(x)}}=\pm\frac{dy}{\sqrt{F(y)}}$$

的积分.

于是, 他的主要关切便是当 F 给出时决定 Φ; 他用待定系数法来做它, 这给了他一个含有一个任意常数的多项式 Φ, 用他的话来说, 即一个对由 F 决定的微分方程的 "完全" (或者通) 积分. 在这里他也包括进了 F 具次数 2 或 1 的情形, 甚至还对此情形写了一整篇文章 (这是个初等的情形, 因为 $dx/\sqrt{F(x)}$ 可以用对数和反三角函数积分出来; 参看 *Eu.*I-20,110–152=E263;1753. 在这情形, 如他所指出的, 只要考虑对 x 和 y 一起为二次的关系式 $\Phi=0$ 就足够了, 即在上面的公式中令 $\varepsilon=\zeta=0$. 他这样做仅仅是将他曾注意到的在 $dx/\sqrt{1-x^4}$ 与 $dx/\sqrt{1-x^2}$ 之间的类比向前推进, 这个类比对于我们来说, 最好解释为他在处理定义在实数域上的各种一维的代数群 (圆当然是其中一种). 然而他真正关心的是 F 为三次或四次多项式的情形, 更特殊的是 F 甚至是一个四次的偶多项式:

$$F(x)=1+mx^2+nx^4.$$

他感觉到一般的情形总可以化成这个. 事实上, 可以通过一个适当的变换

$$x\mapsto\frac{\lambda x+\mu}{\nu x+\rho}$$

做到这一点, 这是他曾要证明的 (*Eu.*I-20,303–304 于 E345 中; 1765); 他的证明仍是不完整的, 这是因为仅仅在复数域上建立了它, 而在他心里想到的明显是实数. 这在后来才被勒让德厘清 (参看他的*Mémoire sur les transcendants elliptiques*,Paris,An II[=1793 年],pp.9–10).

对于 $F(x)=1+mx^2+nx^4$ (或者除了在数论背景下, 等价于 $F(x)=A+Cx^2+Ex^4$), 欧拉发现可以取 Φ 为一个对 x, y 的偶多项式 (对于一个推理性的、对该事实合理性的论证, 可参考附录 III). 于是待定系数法直接地导向了 "完全积分"

$$0=c^2-x^2-y^2+nc^2x^2y^2+2xy\sqrt{1+mc^2+nc^4},$$

其中的 c 是个任意常数 (*Eu.*I-20,67 于 E251 中;1753; *Eu.*I-20,155–159 于 E261 中;1775; *Eu.*I-20,310 于 E345 中;1765), 而后则导向了加法公式 (附录 III 的公式 (3) 和 (4);*Eu.*I-20,69 于 E251 中;*Eu.*I-20,159 于 E261 中; *Eu.*I-20,311 于 E345 中).

1765 年欧拉向前跨了一步, 将待定系数法用来计算一般情形的 "典则方程" $\Phi=0$:

$$F(x)=A+2Bx+Cx^2+2Dx^3+Ex^4.$$

从我们的现代观点看, 这等于是以适当的参数, 定义由 $y^2=F(x)$ 给出的曲线 Γ 的自同构群, 现在它已是为人周知, 这个群等同于 (在定义 Γ 的基域上) 所谓 Γ

的 “雅可比”; 这是一条椭圆曲线

$$Y^2 = 4X^3 - iX - j,$$

它在基域的某个代数扩域上双有理等价于 Γ, 但不一定在它自己的基域上; i, j 只不过是四次多项式 F 的不变量 (譬如参看 A.Weil, *Coll.Papers*.II,111–116). 当然这些概念远远地超出了欧拉的视野. 但是他的计算 (*Eu*.I-20,321–326 于 E347 中;1765; 参看 *Eu*. I-20,71–76 于 E347 中;1753) 包含了隐藏在以上陈述背后的所有事实, 其中有对于不变量 i, j 以 A, B, C, D, E 表达的公式; 这是非凡的成就.

最后必须指出, 在这一节我们仅讨论了欧拉在椭圆积分工作的代数方面. 正由于法尼亚诺在他之前, 欧拉他自己总是非常着重于那些与他的代数结果相伴的积分间的关系. 双纽线、椭圆和双曲线的弧长分别给予他所谓 “第一类” 和 “第二类” 积分的典型例子. 他最终拓展了他的探索甚至到了第三类积分的最一般情形, 即这样一种形式 $\int(Zdz)/\sqrt{F(z)}$, 其中 F 如前, 而 Z 是 z 的任意有理函数 (*Eu*.I-21,39–56=E581;1775). 实际上所有这样的结果只不过是阿贝尔定理 (Abel's theorem) 结合上代数加法公式的特殊情形 (参看附录 III), 故而我们无需在这里走进那个课题里.

§3.16 作为丢番图方程的椭圆曲线

在欧拉从事椭圆函数这个最活跃的课题时的年月里, 他似乎把亏格 1 的丢番图方程搁置在了一旁 (在我们眼里这是紧密相连的). 他只是在 1770 年写他的《代数学》的最后一节时才回到了它. 自那时以后, 那些亏格 1 的以及其他一些簇的丢番图问题成了他最喜爱的娱乐之一.

在 1770 年后写出的 9 篇关于这种主题的文章在他生前得以发表; 24 篇其他的全都写于 1777 年到 1783 年的文章则在其死后才付印. 他在 1772 年写道: “我必须承认, 我从这一类的研究中得到的快乐与从对高等数学的最深入的思索中得到的几乎一样多. 我的确将我大部分的精力投入到具有较大意义的问题上, 但是这样的主题改变总带给了让我欢迎的放松. 另外, 高等分析需要感激丢番图方法是如此之多, 人们没有权利全然抛弃它而不顾” [“*...fateri cogor me ex huiusmodi investigationibus tantundem fere voluptatis capere quam ex profundissimis Geometriae sublimioris speculationibus. Ac si plurimum studii et laboris impendi in quaestionibus. gravioribus evolvendis, huiusmodi variatio argumenti quandam mihi haud ingratam recreationem affere solet. Ceterum Analysis sublimior tantum debet Methodo Diophanteae, ut nefas videatur eam penitus repudiare*”:*Eu*.I-3,174 于E427 中;1772].

初看起来, 这些在欧拉的《*Opera Omnia*》中占了 III, IV 和 V 卷很大篇幅的文章看起来像是一个难做的习题的汇集, 多少有点像随意汇拢的. 人们钦佩欧拉在进行最深奥的计算时的鉴赏力, 或者更钦佩 (由于在那时他几乎全盲) 他对他的助手们处理它们的指挥, 不带感情地引导他们从细节上进行仔细检查. 通过更密切的考察, 人们注意到费马持续地专注于亏格 1 的方程并在他的《代数学》中为它们保留了一个显要的位置 (参看 §5(d)). 在 E405;1770 和 E451;1772 中, 例如 (*Eu.*I-3,148–171 以及 282–296), 一些没有实质性兴趣的问题利用了形如

$$y^2 = A + Bx + Cx^2 + Dx^3 + Ex^4$$

的方程来解决, 其中的 A 和 E 是平方数; 每有机会他都重新叙述费马求这些方程的无穷多个解的方法 (参看第二章 §15; 以及欧拉的《代数学》,*Eu.*I-1,396), 称它们为 "通常方法" ("*methodos consuetas*", *Eu.*I–3,158); 或许在这里他的目的只不过是教会他的助手们这些方法吧. 他反复处理两个费马的著名的问题 (第二章 §15 的问题 (A),(B); 参看同上, §16 以及附录 V), 我们已经看到过, 它们等价于方程 $2X^4 - Y^4 = \pm Z^2$, 或者也等价于 (像欧拉依照莱布尼茨所暗示的那样, 喜欢表述成的) 一对方程 $X + Y = U^2$, $X^2 + Y^2 = V^4$; 1773 年他用下降法粗略地描述了一个解 (*Eu.*I-4,96–98=E560,IV, 发表于 1783 年), 因而在某种程度上抢在了拉格朗日的 1777 年文章中对此课题的决定性的处理 (*Lag.*IV,377–398) 之前; 1780 年, 他引述了拉格朗日的文章, 继续寻求改进他自己和拉格朗日的处理, 但是舍弃使用下降法的新证明依旧是不完全的 (*Eu.* I-5,77–81=E769).

在 1777 年, 还有 1782 年, 他在寻找对于方程 $X^4 + mX^2Y^2 + Y^4 = Z^2$ 及对 "二重方程"

$$X^2 + Y^2 = Z^2, \quad X^2 + NY^2 = T^2$$

具有无穷多个解的判别法 (*Eu.*I-4,235–244=E696;1777;*Eu.*I-5,35–47 =E755;1782; *Eu.*I-4,255–268=E702;1777); 像预料到的那样, 他失败了 (至今仍是个未解决的问题), 但确实得到了非平凡的充分条件. 1780 年, 他将后面的这个问题扩张到二重方程

$$X^2 + mY^2 = Z^2, \quad X^2 + nY^2 = T^2$$

(*Eu.*I-5,48–46=E758;1780); 在这里, 他的以及我们的兴趣要转向去证明对于 $m = 1$, $n = 3$ 或 4 的情形, 还有等价于这两种的其他一些情形的不可解性了; 对于他将无穷下降法 (infinite descent)应用到这些问题上的漂亮技术 (与费马的很不相同), 人们会表达出由衷的钦佩之情.

对我们来说, 更重要的是写于 1780 年的一些文章 (*Eu.*I-5,82–115, 146–181= E772,773,777,778), 其中第一篇具有显示文章特点的标题: "*De insigni promotione*

Analysis Diophanteae" ["论丢番图分析中的一些著名进展":E772]. 与它们一起的还有欧拉关于其他各种课题的文章, 它们全都发表在 1830 年的《*Mémoiris de l'Académie des Sciences de Saint Pétersbourg*》的第 11 卷 (在 1809 年他将它们的拉丁文标题全变成了法文). 就是这篇东西让雅可比有机会写出了他的 1835 年的评注, 该评注的标题也颇具特点: "*De usu theoriae integralium ellipticorum et integralium abelianorum in analysi diophantea*" ["论在丢番图分析中椭圆积分和阿贝尔积分的应用": *Jac.*II,53–55; 参看第二章 §17], 并有机会表达出他的观点, 即欧拉一定已经注意到了形如 $y^2 = F(x)$ 的丢番图方程与椭圆积分 $\int dx/\sqrt{F(x)}$ 之间的关联, 这里的 F 的次数为 3 或 4.

对我们来说, 当知道了方程 $y^2 = 1 + mx^2 + nx^4$ 的两个有理解 (x, y), (a, b) 时, 加法公式 (附录 III 中的 (3) 和 (4)) 决定了它的一个有理解 (x', y') 的确是显然的; 真正令人惊奇的是, 如果欧拉在一再重复写出这些同一个公式以及从它们导出的乘法公式时, 他竟从没有想到过它 (参看 *Eu.*I-20,67,159.311, 以及前面的 §15). 实际上, 他没有给出任何暗示说他感受到了这样的事实; 幸运的是, 他 1780 年的文章给出了他思考方式的一些线索.

我们在 §15 中已经看到, 他处理椭圆积分的方式完全基于他的 "典则方程" $\Phi(x, y) = 0$. 其中 Φ 对 x 和 y 的次数各为 2 . 现在他的 "著名进展" 的文章 E772 中正好在于将这个方程作为椭圆曲线的模型引进来, 以代替这个方程以及以前所使用的 "二重方程". 断言他这样做是充分注意到这两个主题之间的关联似乎被他在新背景中仍使用对方程 $\Phi = 0$ 同样的名称 ("典则方程") (*Eu.*I-5,158 于 E778 中), 以及对它使用完全一样的记号 *Eu.*I-5,153 于 E777 中并对照 *Eu.*I-20,321) 所证实.

在我们看来, 欧拉的 "著名进展" 就是这个关联性的感觉 (后来由雅可比将其清晰表达), 并且这就是使他突然停止考虑下一步进程的那些因素. 当然从另一方面说当问题给出时, 如何得到一个 "典则" 模型的问题便发生了. 代数几何提供了对此的一个准则; 对于给定的一条亏格 1 的曲线 Γ , 有一个模型 $\Phi(x, y) = 0$, 其中 Φ 为对 x 和对 y 都是二次, 当且仅当在 Γ 上存在两个不等价的二次有理除子 (参看第二章, 附录 II). 对于欧拉来说, 该曲线是由方程 $y^2 = F(x)$ 给出的, 要解答的问题是求二次多项式 P, Q, R 使得 $F = P^2 + QR$, 然后可取

$$\Phi(x, y) = Q(x)y^2 + 2P(x)y - R(x)$$

(*Eu.*I-5,158), 他只能靠反复试验来做到. 一旦做到了, 他便使用方程 $\Phi = 0$ 去进行我们称之为的 "提升" (参看第二章,§15), 即由任何已经知道的解去构造新的解, 并恰当地宣称新的方法远比传统的有效率, 而传统的方法不仅 "要求最冗长乏味的计算" 而且 "顷刻间产生出如此大量的数, 使得没有人能够承受得住这

样多的劳作" ["*nimis taediosas ambages requirit...mox ad tam enormes numeros pervenitur, ut vix quisquam tanyum laborem suscipere voluerit*":*Eu*.I-5,82 于 E772 中]. 他的方法 (其例已在前面第二章的附录 V 中给出) 可叙述如下.

如前, 我们写成

$$\begin{aligned}\Phi(x,y) &= P_0(x)y^2 + 2P_1(x)y + P_2(x)\\ &= Q_0(y)x^2 + 2Q_1(y)x + Q_2(y),\end{aligned}$$

其中 P_i, Q_i 为二次多项式. 如果 $M = (x,y)$ 是 $\Phi = 0$ 的一个解则有另一个解 $N = (x,y')$, 其中 y' 由 $y + y' = -2P_1(x)/P_0(x)$ 给出, 或者另一种选择, 由 $yy' = P_2(x)/P_0(x)$ 给出; 于是有一个解 $M' = (x',y')$ 由 $x + x' = -2Q_1(y')/Q_0(y')$ 或者 $xx' = Q_2(y')/Q_0(y')$ 给出. 重复这个步骤, 便得到一个解的无穷序列 M, M', ,M'', M''', $\cdots$, 它们一般来说是互不相同的. 另一个相似的序列由交换 x 和 y 的在此过程中的角色得到.

要了解在这里所进行的, 最好运用在第二章附录 II 中所解释的概念. 在由 $\Phi = 0$ 定义的亏格 1 的曲线上设 A, A' 为使 $x = \infty$ 的点, B, B' 为使 $y = \infty$ 的点; 令 $\mathfrak{a} = A + A'$, $\mathfrak{b} = B + B'$; 它们分别是 x 和 y 的极除子; 因此它们是有理的. 在上面的记号下, x 在 M 和在 N 的取值相同, 故而我们有 $M + N \sim \mathfrak{a}$; 相似地, 我们有 $N + M' \sim \mathfrak{b}$. 于是, 令 $\mathfrak{m} = \mathfrak{b} - \mathfrak{a}$, 我们便有 $M' \sim M + \mathfrak{m}$, 从而相似地, $M'' \sim M + 2\mathfrak{m}$, $M''' \sim M + 3\mathfrak{m}$, 等等. 现代关于高的理论表明这个序列的第 n 个点的高, 即用来表达它的坐标的整数的大小 (参看第二章附录 IV), 具有量级 n^2, 对照于由 "传统方法" 产生的那些点, 由于那些方法依赖于倍量公式, 故它们的高以指数式增长. 这便解释了欧拉的发现.

§3.17　求和公式以及 $\sum n^{-\nu}$

[为简便起见, 我们将记级数 $\sum_1^\infty n^{-s}$ 为 $\zeta(s)$, 或者更准确地, 像欧拉那样将其表示为

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots,$$

以 $L(s)$ 表示 $\sum_0^\infty (-1)^n (2n+1)^{-s}$ 或者

$$1 - \frac{1}{3^s} + \frac{1}{5^s} - \cdots,$$

以及以 $n!$ 表示 $1 \cdot 2 \cdot 3 \cdot \ \cdots \ \cdot n$].

在欧拉还是约翰 · 伯努利的学生那个时候, 当 n 为 ≥ 2 的整数时的级数 $\zeta(n)$ 的求和是一个经典问题, 它们曾使莱布尼茨和伯努利兄弟得到锻炼 (参看 *Corr*.II,15;1737). 在 1647 年, $L(1)$ 的求和或许是年轻的莱布尼茨最令人印象深

刻的早期发现了 (按惠更斯预言, 这是在几何学家中 "永垂其名的" 一个发现: *Huy.*VII,394;1674), 但是它有赖于幂级数展式

$$\arctan x = \frac{x}{1} - \frac{x^3}{3} + \frac{x^5}{5} - \cdots,$$

这给出了 $L(1) = \pi/4$; 这既不能推广到对任意 $n > 1$ 的 $\zeta(n)$ 也不能推广到 $L(n)$. 甚至这些级数的数值估值, 由于它们的慢收敛性也不是个普通的问题.

我们发现在 1728 年, 丹尼尔 · 伯努利写信给哥德巴赫说级数 $\zeta(2)$ "非常接近 $\frac{8}{5}$" (*Corr.*II,263;1728); 哥德巴赫用初等的方法回答说 $\zeta(2) - 1$ 介于 16223/25200 于 30197/46800 之间 (因而在 0.6437 与 0.6453 之间: *Corr.*II,282;1729). 那时欧拉已在彼得堡, 每日与丹尼尔接触; 他必定已注意到了这些信件. 不久他就递交给科学院一篇文章, 以对 $\zeta(2)$ 的一个更好的估值 1.644934 作为结束, 这是他以对积分计算的灵巧运用得到的 (*Eu.*I-14,41 于 E20 中;1731).

毫无疑问, 这些以及类似的问题给予欧拉所谓的 "欧拉–麦克劳林求和公式" (它被麦克劳林独立地发表在他的《流数论 (*Treatise Fluxions*)》, Edinburgh,1742 中) 的发现以强有力的启示. 这在 1732 年提交给科学院的文章中已有陈述 (*Eu.*I-14,42–72=E25). 三年以后, 他给出了一篇对此问题进行了充分陈述的文章 (*Eu.*I-14,108–123=E47;1735, 参看 *Eu.*I-14,435–439 于 E130 中;1739, 以及他的《*Institutiones Calculi Differentialis*》中的第五章, 1775, Part II,*Eu.*I-10,309–336). 他的方法可总结于下.

他明白该问题是要找到一个求和 $\sum f(i)$ 的一个公式. 该和取于 $1 \le i \le n$, $f(x)$ 是我们称之为的 x 的对所有 $x > 0$ 的解析函数; 由此要推导出 $\sum_1^\infty f(i)$ 的值. 答案在形式 $S(n)$ 中寻找, 这里的 S 也是 $x > 0$ 的解析函数. 明显的是, 如果 S 满足差分方程

$$S(x) - S(x-1) = f(x)$$

且 $S(0) = 0$, 或者至少如果某个整数 ν, 它满足 $S(\nu) = \sum_1^\nu f(i)$, 那么这个 S 便是我们需要的. 至于这个差分方程, 欧拉用泰勒 (Taylor)定理 (他在这里指的是 1715 年泰勒所发表的, 尽管他必定也知道在此之前已由莱布尼茨和约翰 · 伯努利得到; 参看 *Eu.*.I-14,109), 将它重写为形式

$$f(x) = \frac{dS}{dx} - \frac{1}{2!}\frac{d^2S}{dx^2} + \frac{1}{3!}\frac{d^3S}{dx^3} - \cdots,$$

并令

$$S(x) = \alpha \int f dx + \beta f + \gamma \frac{df}{dx} + \delta \frac{d^2 f}{dx^2} + \cdots$$

来解出它, 其中 α, β, γ 等为待定系数; 这些数将用把这个试探性的公式代回到前面的方程中并使两端恒等来决定. 这个加上的常数隐含在不定积分 $\int f dx$ 中

可以由取 x 的一个任意值而确定, 譬如取 $x=0$. 这立即让他用递归公式得到了 α, β, γ 等的值; 他得到了 $\alpha=1$, $\beta=1/2$, 然后, 譬如

$$\delta=\frac{\gamma}{2!}-\frac{\beta}{3!}+\frac{\alpha}{4!},$$

等, 从而 (但 "以大量的工作"["*multo labore*"]:*Eu.*I-14,436) 得到前 14 个系数的数值; 那些除 β 以外偶数阶的项原来全为 0.

在此欧拉说它是按照 "一个已知方法" ("*methodo cognita*":*Eu.*I-14,112) 进行的, 对于它他很可能说的是待定系数 "法". 实际上, 他是大胆到了轻率的程度; 但是正如拉丁谚语所说 "*audaces fortuna iuvat* (幸运偏爱大胆)". 形式地说, 他的方法可用算子 $D=d/dx$ 澄清; 于是我们可以写出

$$S(x-1)=e^{-D}S(x),\ f(x)=S(x)-S(x-1)=(1-e^{-D})S(x)$$

以及, 自然是形式的,

$$S(x)=(1-e^{-D})^{-1}f(x)=(\alpha D^{-1}+\beta+\gamma D+\delta D^2+\cdots)f(x),$$

其中 α, β, γ 等现在是作为 $z/(1-e^{-z})$ 在 $z=0$ 处的泰勒展示的系数出现的 (*Eu.*I-14,436 于 E130 中;1739). 从这个最初从欧拉眼皮下溜走的事实, 容易推导出在上面公式中的偶次幂的系数全为 0, 这与他早先的计算相吻合 (参看同前). 如果现在令

$$\frac{z}{1-e^{-z}}=\sum_{m=0}^{\infty}\frac{1}{m!}b_m z^m,$$

便得到 $b_0=1$, $b_1=\dfrac{1}{2}$, $b_{2m-1}=0, m>0$; 至于 b_{2m}, $m>0$, 它们逐次的值等于

$$\frac{1}{6},-\frac{1}{30},\frac{1}{42},-\frac{1}{30},\frac{5}{66},-\frac{691}{2730},\cdots;$$

而欧拉的结果形式上说等于是公式

$$(EM)\qquad S(x)=\sum_{i=1}^{\nu}f(i)+\int_{\nu}^{x}f(t)dt+\sum_{m=1}^{\infty}\frac{1}{m!}b_m\left[f^{(m-1)}(x)-f^{(m-1)}(\nu)\right],$$

其中对于 $i\geq 0$ 的 $f^{(i)}$ 表示 f 及其逐次导数.

欧拉立即看出 (*Eu.*I-14,43–44 于 E25 中;1732;*Eu.*I-14,115–117 于 E47 中; 1735), 这个结果当 $f(x)$ 为 x 的多项式时总有效. 于是上面给出的对 $S(x)$ 的级数化成了有限和从而定义了差分方程 $S(x)-S(x-1)=f(x)$ 的一个多项式解. 例如, 取 $f(x)=x^r$, $r\geq 1$, 且 $\nu=0$, 我们便有

$$1^r+2^r+\cdots+n^r=S_r(n),$$

其中 S_r 是由

$$S_r = \frac{x^{r+1}}{r+1} + \frac{x^r}{2} + \sum_{1 \le m < \frac{r+1}{2}} \binom{r}{2m-1} \frac{1}{2m} b_{2m} x^{r+1-2m}$$

(*Eu.*I-14,116–117) 给出的多项式, 或者更简单地, 由

$$\frac{dS_r(x)}{dx} = B_r(x) = \sum_{m=0}^{r} \binom{r}{m} b_m x^{r-m}, \quad S_r(0) = 0$$

给出.

这个结果部分地被费马所预料到 (参看前面的第二章 §2), 并更全面地被雅各布 · 伯努利预料到 (参看他身后的 1713 年在巴塞尔出版的《猜度术 (*Ars Conjectandi*)》, pp.96–97); 后者的优先权最终得到欧拉的认可, 他也采纳了棣莫弗对数 b_{2m} 命名的 "伯努利数" (参看 A.de Moivre,《*Miscellanea Analytica*》, Londini 1730, Complementum,pp.6 以及 19–21); 欧拉写道:"这些数依照它们的发明人的名字成为伯努利数, 这是因为他在他的《*Miscellanea Analytica*》中把它用到了自然数的幂次和上了"["*numeri ab inventore Bernoulliani vocati, quippe quibus olim Jacobus Bernoulli in Ars Conjectandi est usus ad progressiones potestatum numerorum naturalium summandas*": *Eu.*I-15,92 于 E393 中;1768; 参看在他 1755 的《*Institutiones Calculi Differentialis*》中类似的评论,*Eu.*I-10,321].

在这个时刻欧拉心中首要关心的是像 $\zeta(n)$, $n = 2, 3, 4$ 等这些级数的数值估值, 并也从级数 $\zeta(1)$ 的部分和开始着手. 在这种情形一个现代的分析学家会立刻说, 求和公式 (*EM*) 失效了, 这是因为 (欧拉自己看出来了: *Eu.*I-14,357 于 E125 中;1739; 参看 *Eu.*I-14,119 于 E47 中;1753, 以及在《*Institutiones Calculo Differentialis*》中的段落 *Eu.*I-10,327) 数 $|b_{2m}|$ 增大的如此之快以致所涉及的级数总是发散的. 为数值计算的目的使用它们的正确方法是把它们截断成有限和然后估计余项. 不同于此的欧拉的方法是加这些项 "直到它们开始发散" ("*quoad termini divergere incipiant*":*Eu.*I-14,357); 或许人们更应该说他让自己跟着他的本能走 (确实在这方面不是一个坏的导向). 于是他可以计算 $\zeta(2)$ 到 20 位小数

$$\zeta(2) = 1.64493406684822643647 \cdots,$$

$\zeta(3)$ 到 15 位, $\zeta(4)$ 到 16 位, 所谓的 "欧拉数" 到 16 位 (*Eu.*I-14,119–122 于 E47 中;1735), 然后 π 到 15 位 (*Eu.*I-14,359 于 E125 中;1739); 最终他用这样的方法去计算 $\zeta(n)$, $2 \le n \le 16$ 到 18 位数 (*Corr.*I,207;1743; 参看 *Eu.*I-14,440 于 E130 中;1739, 以及他 1748 年《*Institutiones Calculo Differentialis*》的第 XI 章; 参看 *Eu.*I-8,201–205). 毫无疑问, 即便没有理论性的结论, 他也从这些计算中获得了很大的乐趣, 当然有时他是能够从它们中提取出理论的.

§3.18 欧拉和 ζ 函数

在 1735 年欧拉曾写道 "对于有关级数 $\zeta(n)$ 已经做了如此多的工作, 以至于似乎很难有望出现什么有关它们的新东西了…… 我也是, 不管怎样反复努力只不过在对它们和的近似值方面取得些成果…… 但是现在十分出乎意料地, 我发现了对 $\zeta(2)$ 的一个漂亮公式, 他依赖于圆的求积 [即依赖于 π]" [“*Tantopere iam pertractatae et investigatae sunt series reciprocae potestatum numerorum naturalium, ut vix probabile videatur de iis novi quicquam inveniri posse...Ego etiam iam saepius...has series diligenter sum persecutus neque tamen quicquam aliud sum assecutus, nisi ut earum summam...proxime veram definiverim...Deductus sum autem nuper omnino inopinado ad elegantem summae huius seriei* $1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+$ etc. *expressionem, quae a circuli quadratura pendet*":*Eu.*I-14,73–74 于 E41 中;1735].

当他写这段话时, 显然他刚发现了他的著名结果 $\zeta(2)=\pi^2/6$. 他关于这个主题和其他各种与其紧密相关的求和的文章于 1735 年 12 月 5 日递交给了科学院; 直到 1740 年方才发表 (*Eu.*I-14,73–86=E41), 但是在那时只要算作是国际数学界的每个人都会被知会到: 或许首先是欧拉在巴塞尔的朋友丹尼尔 · 伯努利 (参看 *Corr.*II,435;1736 年 9 月 12 日, 以及 *Corr.*II,15–16;1737); 还有爱丁堡的斯特林 (Stirling)*[11] (*Eu.*IV A-1,no.2621;1736 年 6 月 8 日), 但泽的 Ehler 和 Kühn (*PkU.*345;1736 年 4 月 3 日), 帕多瓦的珀勒利*[12](*PkU.*216;1736 年 3 月 13 日), 柏林的 Naudé (*PkU.*193–199;1740), 以及直接的或通过上面这些人得到的, 其中当然包括了约翰 · 伯努利 (参看 *Corr.*II,15–16;1737). 至于哥德巴赫, 在此发现的当时就在彼得堡, 肯定立刻就知道了. 1742 年当得知克莱罗对此事没有得到充分的信息时, 欧拉便迅速地给他送去了完整的细节, 在前面写下了这样的话:“*Mr. Jacq. Bernoulli...parle de ces suites, mais...il avouë, que malgré toutes les peines, qu'il s'etoit données ,il n'avoit pû venir à bout, de sorte que Mrs.* [Jean] *Bernoulli, de Moivre et Stirling, grands Maitres dans cette matiee, ont été extrêmement surpris, quand je leur annonçois que j'avois trouvé la somme de cette serie*

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\text{etc.}$$

et même de celle-ci

$$1+\frac{1}{2^n}+\frac{1}{3^n}+\frac{1}{4^n}+\frac{1}{5^n}+\text{etc.}$$

*[11] 1692—1770, 苏格兰数学家, 以斯特林数和斯特林近似而知名.

*[12] (Poleni) 1683—1761, 意大利数学家, 其领域包括水力学, 物理, 天文和考古.

quand n est un nombre pair"["雅各布 · 伯努利确实提到了那些级数, 但是承认, 不管他多努力也没能做出来. 所以约翰· 伯努利、棣莫弗和斯特林等这些方面的权威们在我告诉他们我已找到了 $\zeta(2)$ 的和甚至 n 为偶数时 $\zeta(n)$ 的和时, 他们非常惊讶":*Eu*.IV A-5,120]. 这些几乎与费马曾用来形容他自己的一个发现时的话完全一样 ("*c'est une de mes inventions qui a quelquesfois estonné les plus grands maistres*: 参看第二章§15). 从 1736 年往后, 以及下一个 8 到 10 年, 欧拉的结果及他的证明的可信度成了他与朋友们和整个欧洲同事们通信中的周而复始的话题.

在这里欧拉有一次显得莽撞, 他将牛顿的关于代数方程根的 n 次幂之和的定理用到了形如 $y = \sin s$ 的超越方程上, 其中的 y 给定, s 为未知. 运用 sin 的幂级数并记 A, B, C 等为该方程的根, 他将其写成

$$\begin{aligned}0 &= 1 - \frac{s}{y} + \frac{s^3}{1\cdot 2\cdot 3\cdot y} - \frac{s^5}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot y} + \cdots \\ &= \left(1-\frac{s}{A}\right)\left(1-\frac{s}{B}\right)\left(1-\frac{s}{C}\right)\cdots,\end{aligned}$$

并由此首先得到

$$\frac{1}{y} = \frac{1}{A} + \frac{1}{B} + \frac{1}{C} + \cdots,$$

然后比较 s^2 项, 有

$$0 = \frac{1}{AB} + \cdots = \frac{1}{2}\left(\frac{1}{A} + \frac{1}{B} + \cdots\right)^2 - \frac{1}{2}\left(\frac{1}{A^2} + \frac{1}{B^2} + \cdots\right),$$

这给出了 $\sum 1/A^2 = 1/y^2$, 以及对高次幂的相似结果. 特别取 $y = 1$, 他说根 $A, B, C, \cdots$ 为 $q, q, -3q, -3q, 5q, 5q, \cdots$, 其中的 q 是半径为 1 的圆的周长的四分之一 (即 $\pi/2$, 这是他很快就要采用的记号). 它给出了

$$1 = 2 \times \frac{2}{\pi}\left(1 - \frac{1}{3} + \frac{1}{5} - \cdots\right),$$

这是莱布尼茨的结果, 进一步有

$$1 = 2 \times \left(\frac{2}{\pi}\right)^2 \left(1 + \frac{1}{3^2} + \frac{1}{5^2} + \cdots\right).$$

当然对欧拉来说显然有

$$\begin{aligned}1 + \frac{1}{3^2} + \frac{1}{5^2} + \cdots &= \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right) - \left(\frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \cdots\right) \\ &= \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right)\left(1 - \frac{1}{2^2}\right) = \frac{3}{4}\zeta(2),\end{aligned}$$

所以上面最后部分给出了 $\zeta(2) = \pi^2/6$. 同样的方法更进一步便给了欧拉 (多少有点费劲, "*multo labored*":*Eu.*I-14,85) $\zeta(n)$ 对于 $n = 4, 6, 8, 10, 12$ 的值, 以及 $L(n)$ 对于 $n = 3, 5, 7$ 的值. 将它应用于 y 的不同于 $y = 1$ 的值, 它仍可给出其他一些级数的值 (用现代术语即狄利克雷级数). 所有这些都在欧拉 1735 年的文章中被迅速概述; 人们几乎可以感受到这位作者的狂热激情.

欧拉的方法公开面对着这严重的反对意见, 他自己甚至当在他的通信中被指出时就已感觉到了 (参看 *Eu.*I-14,79 于 E41 中;1735 以及 *Eu.*I-14,139–140 于 E61 中;1743), 这些通信包括了与约翰 · 伯努利 (参看 *Corr.*II,16–17) 的, 同样还有与丹尼尔 · 伯努利的 (参看*Corr.*II,477;1741), 丹尼尔的哥哥尼古拉斯 · 伯努利的 (参看*Corr*II,683;1742), 在日内瓦的克莱姆 (Cramer)*[13] 的, 或许还有其他人的. 除了对所涉及的级数的收敛性, 或可能还有发散性 (一个由尼古拉斯 · 伯努利提出的多少有点笨拙的提问: *Corr.*II,683–684 和 691;1742) 问题外, 人们还可以有理由问道, 是否超越方程

$$1 = s - \frac{1}{1 \cdot 2 \cdot 3} s^3 + \cdots$$

在它的 "看得见" 的实根以外还有其他的 "虚根", 如果这样它将损害整个计算 (*Corr.*II,16; 参看 *Eu.*IV A-5,121); 即便在欧拉对于变量的那些虚根上定义了 sin 的值之前, 这种提问还有些意义, 这种反对意见也不只是限于形如 $a + b\sqrt{-1}$ 这种根的存在问题 (参看下文的 §19); 对于处于代数方程至少有一个表面看似正确的猜想式的所谓代数基本定理 (参看前面的 §7) 甚至不能合理地规定一个诸如欧拉试图处理的 "无穷次" 方程. 更为特殊地, 一个作为反对他的理由是, 如果把在几何中定义正弦的圆替换成椭圆, 虽然他的方程的所有看得见的实根仍旧保持一样, 但他的结论显然是错误的 (*Corr.*II,477).

最初欧拉观察到他的方法的与莱布尼茨的在 $L(1)$ 情形的结果是一致的 (所以, 如他所说, 如果方程 $1 = \sin x$ 除看得见的实根外还有 "虚" 根, 则至少它们的倒数和会为 0), 所以他暂时把他的疑虑搁置一旁, 并且还把他的 $\zeta(2)$, $\zeta(4)$ 等新值与他以前曾计算过的数值进行了比较 (参看前面的 §17). 因此他说 "我曾毫不犹豫地发表了这些完全正确的和数" ["*non dubitavi istas summas tanquam verissimas producere*":*Eu.*I-14,140 于 E61 中;1743].

然而, 下一个十年里, 欧拉从没有放松努力, 要把他的结论置于一个完善的基础之上. 首先这只把他引向对 $\zeta(2) = \pi^2/6$ (或者更可以对等价的结果 $1 + 1/3^2 + 1/5^2 + \cdots = \pi^2/8$) 给出一个分析的证明, 但这个证明似乎甚至不能推广到 $\zeta(4)$ (参看他 1737 年给约翰 · 伯努利的信, *Bibl.Math.* (III) 5 (1904),pp.258–259, 以及 P. Stäckel 的文章, *Eu.*I-14,156–176). 然而现在他的注意力被他 1735

*[13] 1704—1752, 瑞士数学家, 以克莱姆法则与克莱姆悖论知名.

年的具启发性的证明同样还有他早期关于我们现在称之为 Γ 函数的工作引向了与无穷级数相关联的无穷乘积上了, 这也将它引向了一个具纪念碑意义的发现. 在提交给科学院的 1737 年的一篇文章里 (*Eu.*I-14,216–244=E72), 欧拉讨论了一些由哥德巴赫向他提出的相当古怪的级数之后, 继续考虑一些 "同样美妙" 的无穷乘积, 他说道, " 因为在它们中的因子是按照素数来进行的, 而它们的运行(与在哥德巴赫的那些级数的项) 同样不规则" [" *...neque minus erunt admirabilia ...cum...in his...termini progrediantur secundum numeros primos, quorum progressio non minus est abstrusa*":*Eu.*I-14,227]. 他在此的意思是指著名的关于 $\zeta(s)$ 的 "欧拉乘积 (eulerian product)":

$$\zeta(s) = \prod_p (1-p^{-s})^{-1},$$

取所有的素数 p, 或者用他的记号为

$$1+\frac{1}{2^n}+\frac{1}{3^n}+\frac{1}{4^n}+\cdots = \frac{2^n\cdot 3^n\cdot 5^n\cdot 7^n\cdot\ \cdots}{(2^n-1)\cdot(3^n-1)\cdot(5^n-1)\cdot(7^n-1)\cdot\ \cdots}$$

(*Eu.*I-14,230), 以及相似的乘积

$$\frac{\pi}{4} = 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\cdots = \frac{3\cdot 5\cdot 7\cdot 11\cdot 13\cdot\ \cdots}{4\cdot 4\cdot 8\cdot 12\cdot 12\cdot\ \cdots}$$

或者用现代的记号有

$$L(1) = \prod_{p\neq 2}\frac{p}{p\pm 1},$$

其中符号由 $p\pm 1\equiv 0 \pmod 4$ 决定 (*Eu.*I-14,233; 参看 *Corr.*I,577–578;1752). 由前面的那个结果他推导出和 $\sum 1/p$ 为 "像调和级数和 $\sum 1/n$ 的对数那样" 的无穷; 欧拉知道和 $\sum_1^N 1/n$ 数量级为 $\log N$ (譬如参看 *Eu.*I-14,87–100=E43;1734), 这表明和 $\sum_{p<N} 1/p$ 的数量级为 $\log\log N$. 从关于 $L(1)$ 的结果他后来得到的结论是, 和 $\sum_{p\neq 2} \pm 1/p$ (其符号像前面那样决定, 并且奇素数是按大小的递增排列) 是一个有限值, 近似地为 0.334980 (*Corr.*I,587;1752; 参看 *Eu.*I-4,146–153 于 E596 中;1775). 从这些观察显然可推出和 $\sum 1/p$ 历经所有形如 $4n+1$ 的素数, 以及相似的和历经所有形如 $4n-1$ 的素数, 都为无穷并具有同样的数量级.

引进了 "欧拉乘积" 后的一些年, 欧拉在他的《无穷分析导论》中用了一整章 (第 XV 章 =*Eu.*I-8,284–312) 来写这个课题, 在其中他不仅用了几乎现代的形式写了 $\zeta(s)$ 和 $L(s)$ 的乘积表示, 譬如对 $\zeta(n)$ 写出如下的表达式

$$\frac{1}{\left(1-\frac{1}{2^n}\right)\cdot\left(1-\frac{1}{3^n}\right)\cdot\left(1-\frac{1}{5^n}\right)\cdot\left(1-\frac{1}{7^n}\right)\cdot\ \cdots},$$

而且将其推广到了我们现在称其为具狄利克雷模 3 特征标 (*Eu.*I–8,308–309) 和模 8 特征标 (*Eu.*I–8,310–311) 的 L- 级数. 他甚至证明利用前面第 X 章的结果, 可以对这样的级数 (以及 “不可数的其他级数”) 的 $n=1$ 情形求和 (参看下文的 §19). 人们可以将这些研究看成是解析数论诞生的标记.

§3.19 三角函数

1735 年, 欧拉已经能够给出使自己和他的同事们完全满意的他关于 $\zeta(2n)$ 结果的证明了. 1745 年他已经以手稿形式完成了他的《无穷分析导论》, 在其第 VIII 到 XI 章中给出了对于三角函数的理论及其级数和乘积展开式的精巧熟练的阐述 (*Eu.*I-8,133–212), 其中以上面所考虑的这些结果作为它的主要应用之一. 其中的一些以前已在柏林出版 (*Eu.*I-14,138–155=E61;1742); 它的大多数结果显然在欧拉到柏林居住的第一年或第二年就已被发现 (参看 *Eu.*IV A–5,115,120–124,1742 以及 *Corr.*I,131–132;1742).

从他年轻时起他就已知道 e^x 是 $(1+x/n)^n$ 当 $x\to\infty$ 时的极限 (这时他选取的表达方式是写成 “对 n 无穷” (“*existente n numero infinito*”:*Eu.*I-14,143 于 E61 中;1742; 参看他的《无穷分析导论》,*Eu.*I-8,132,147, 等)

$$e^x=\left(1+\frac{x}{n}\right)^n.$$

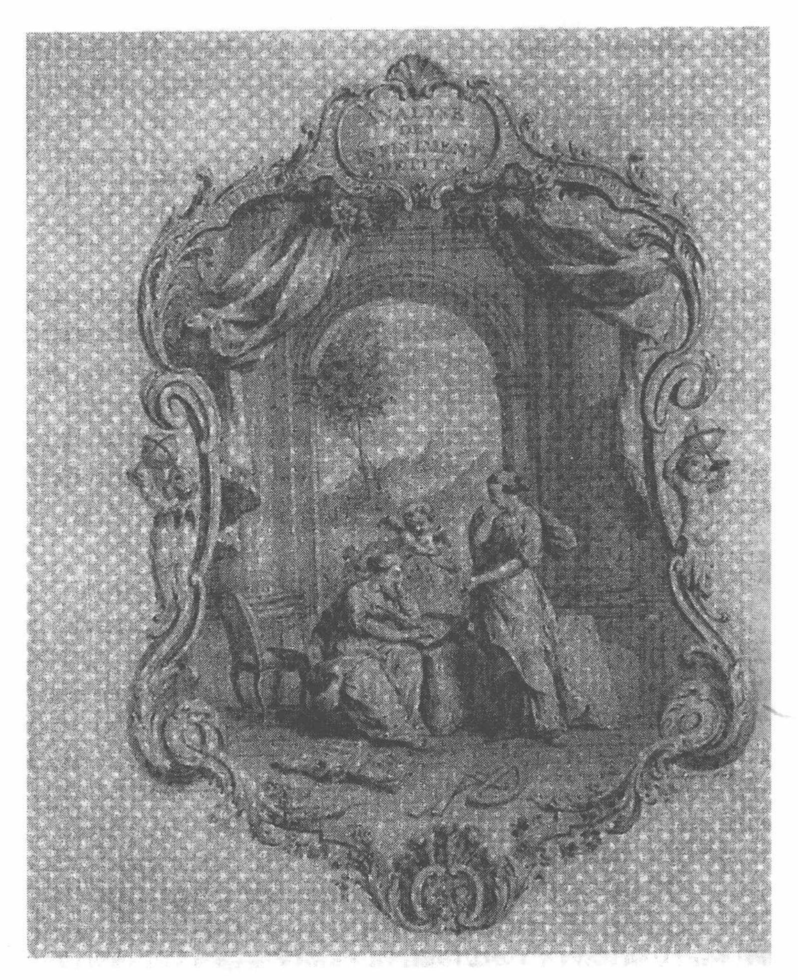
他也熟悉 e^x, $\sin x$, $\cos x$ 的幂级数; 特别他知道 e^x 的幂级数可以用二项式公式展开当 n 为 (有限) 整数时的 $(1+x/n)^n$, 然后再逐项地取 $n\to\infty$ 时的极限 (或者他宁愿将 n 替换为无穷大数: *Eu.*I-8,123–124).

1740 年在与约翰 · 伯努利关于常系数线性微分方程求解问题 (所讨论问题之一) 的信件交换中, 他第一次陈述了著名的公式

$$2\cos x=e^{x\sqrt{-1}}+e^{-x\sqrt{-1}},$$

这是从两端的幂级数展式之间的恒等推导出来的 (*Bibl.Math.*(III)6 (1905), pp.76–77); 他隐含地使用了 e^x 的幂级数展式以便拓展它的定义到变量的复数值. 对于 $\sin x$ 的相似公式当然一定在同时被发现 (参看 *Eu.*I-14,142,144 于 E61 中;1742). 将此结合上面对 e^x 的公式, 欧拉于是可以得出结论说 $\sin x$ 是 $n\to\infty$ 时 (或者如他所说, “ n 的值无穷大”) 多项式

$$P_n(x)=\frac{1}{2\sqrt{-1}}\left[\left(1+\frac{x\sqrt{-1}}{n}\right)^n-\left(1-\frac{x\sqrt{-1}}{n}\right)^n\right]$$



《无穷分析导论 (*Introductio in Analysin Infinitorum*)》的卷首插图页

INTRODUCTIO

IN ANALYSIN

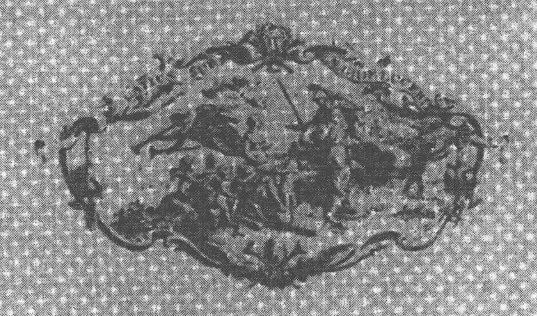
INFINITORUM.

AUCTORE

LEONHARDO EULERO,

Professore Regio BEROLINENSI, *& Academiæ Imperialis Scientiarum* PETROPOLITANÆ *Socio.*

TOMUS PRIMUS.



LAUSANNÆ

Apud MARCUM-MICHAELEM BOUSQUET & Socios.

MDCCXLVIII.

《无穷分析导论 (*Introductio in Analysin Infinitorum*)》的扉页

的极限. 现在 P_n (如他所说, 对 n 有限) 容易被分解成它的次数为 1 和 2 的实因子 (参看前面的 §7). 对于一个奇数 $n=2p+1$, 这可用恒等式实现:

$$X^n - Y^n = (X-Y)\prod_{\nu=1}^{p}(X - e^{+2\pi i\nu/n}Y)(X - e^{-2\pi i\nu/n}Y)$$
$$= (X-Y)\prod_{\nu=1}^{p}\left(X^2 - 2XY\cos\frac{2\pi\nu}{n} + Y^2\right).$$

这又对 $n=2p+1$ 给出了

$$P_n(x) = x\prod_{\nu=1}^{p} Q_{n,\nu}(x), \qquad Q_{n,\nu}(x) = 1 - \frac{1+\cos\dfrac{2\pi\nu}{n}}{1-\cos\dfrac{2\pi\nu}{n}}\cdot\frac{x^2}{n^2}.$$

可清楚看出, 对任意给定的 ν 以及 " 对 n 无穷大", $Q_{n,\nu}$ 成为 $1-x^2/\nu^2\pi^2$; 由此欧拉得出结论:

$$\sin x = x\prod_{\nu=1}^{\infty}\left(1 - \frac{x^2}{\nu^2\pi^2}\right),$$

以及相似的一个计算给了他对于余弦的一个相应的无穷乘积:

$$\cos x = \prod_{\nu=0}^{\infty}\left(1 - \frac{4x^2}{(2\nu+1)^2\pi^2}\right)$$

(*Eu*.I-14,141–146 于 E61 中;1742; 参看《无穷分析导论》, 第 IX 章 =*Eu*.I-8, 153–176), 用他自己的话说, 证明了他以前用来计算级数 $\zeta(2)$, $\zeta(4)$ 等的无穷次方程, 除去看得见的实根外, "的确没有其他的根了". 我们在前面已注意到, 所有这些都被欧拉使用了 "无穷大的数" 以及 "无穷小的数" 这些语言来表达 (这种语言在我们的年代里又被从事称作 "非标准分析" 的人们复活). 从我们当今的观点看, 当然并没有对他采用这类语言进行推理的合法性评估; 然而就目前这种情形而言, 任何一个初学者都能容易将它们补充好.

正如尼古拉斯 · 伯努利正确地观察到 (*Corr*.II,689;1742; 参看同上, p.694) 由这些无穷乘积可以立即用对数微分推出更进一步的公式, 诸如

$$\frac{\pi\cos\pi x}{\sin\pi x} = \frac{1}{x} + \sum_{\nu=1}^{\infty}\left(\frac{1}{\nu+x} - \frac{1}{\nu-x}\right),$$

欧拉将它写成

$$\frac{\pi\cos\pi x}{\sin\pi x} = \frac{1}{x} - \frac{1}{1-x} + \frac{1}{1+x} - \frac{1}{2-x} + \frac{1}{2+x} - \frac{1}{3-x} + \cdots$$

(在我们看来没有括号应保证该级数绝对收敛). 将此结合可从 $\cos x$ 的乘积推出的公式, 便得到用欧拉记号表示的

$$\frac{\pi}{\sin \pi x} = \frac{1}{x} + \frac{1}{1-x} - \frac{1}{1+x} - \frac{1}{2-x} + \frac{1}{2+x} + \frac{1}{3-x} - \frac{1}{3+x} - \cdots$$

(譬如参看 *Eu.*I-14,148). 欧拉对此有两个其他证明, 一个基于积分计算 (*Eu.*I-14,146–148 于 E61 中;1742; 参看他给克莱罗的信, *Eu.*IV A-5,115;1742), 另一个则直接建立在从上述无穷乘积到形如函数 $\cos x + \cos a$, $\sin x + \sin a$ 的扩张基础之上 (*Eu.*I-8,170–176, 以及《无穷分析导论》, 第 IX–X 章的 184–187). 由此经反复微分不仅容易推导出对于 $n > 0$ 为偶数的 $\zeta(n)$ 的值, 以及对奇数 $n > 0$ 的 $L(n)$ 的值, 而且还有无穷多个其他 (如我们现在所叫的) "狄利克雷级数" 的值 (譬如参看 *Corr.*I,132;1742 或者 *Eu.*I-14,151–152). 特别可以发现 $\zeta(n)$ 对所有偶数 $n > 0$, 有 $r(2\pi)^n$ 的形式, 以及对所有奇数 $n > 0$, $L(n)$ 有 $s(2\pi)^n$ 的形式, 其中的 r, s 为有理数.

第一眼看起来, 在这些结果与欧拉–麦克劳林公式之间没有联系. 但是不久欧拉便不得不十分注意到他在 1735 年已经计算到

$$\zeta(12) = \frac{691\pi^{12}}{6825 \times 93555}$$

的 $\zeta(2n)$ 的值 (*Eu.*I-14,85 于 E41 中;1735) 与出现在他求和公式的工作中的数 b_{2n} (那时他还没称它为伯努利数)之间的关系 (参看 *Eu.*I-14,114 于 E47 中;1735); 特别是不寻常的素数 691 (貌似伯努利数的 "追踪器") 在 $\zeta(12)$ 和 b_{12} 中同时出现不能不对他的思想产生冲击. 一旦看清了这点, 欧拉便没有困难地建立了一个普遍关系

$$\zeta(2n) = \frac{1}{2}(-1)^{n-1}\frac{b_{2n}}{(2n)!}(2\pi)^{2n}$$

(*Eu.*I-14,434–439 于 E130 中;1739).

§3.20 ζ 函数的函数方程

对于奇数 $n > 1$ 的 $\zeta(n)$ 的值仍然保持着它的秘密未被揭开; 的确直到今天它依然如故. 当然已知 $\zeta(s)$ 与交错级数

$$\varphi(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

经由公式

$$\varphi(s) = \left(1 - \frac{2}{2^s}\right)\zeta(s),$$

相关联. 欧拉显然地想到了首先要研究从属于对于奇数 $m>0$ 的发散交错级数 (根据他关于发散级数的观点: 参看 *Eu.*I-14,585–617=E247;1746, 以及他 1755 年《*Institutiones Calculi Differentialis*》中的段落 *Eu.*I-10,81–82)

$$\varphi(-m)=1-2^m+3^m-4^m+\cdots$$

的值 (参看 *Eu.*I-14,443 于 E130 中;1739). 对于他, 这可以用取 $\varphi(-m)=R_m(1)$ 来做到, 其中的 R_m 是一个由级数

$$R_m(x)=1-2^m x+3^m x^2-4^m x^3+\cdots$$

定义 (如人们现在会坚持主张的那样, 对于 $|x|<1$) 的有理函数. 如他所说, "微分学给了我们容易求这些级数和的方法"["*Le calcul différentiel nous fournit un moyen fort aisé de trouver la somme de ces séries*": *Eu.*I-15,71 于 E352 中;1749]. 事实上, 有 $R_0(x)=1/(1+x)$, 并且, 对于每个整数 $m\geq 0$:

$$R_{m+1}(x)=\frac{d}{dx}[xR_m(x)],$$

所以, 对于 $m>0$, R_m 具有形式

$$R_m(x)=\frac{P_m}{(1+x)^{m+1}},$$

其中 P_m 是个次数为 $m-1$ 的整系数多项式. 另外, 就像欧拉必定会做的那样, 对几个 m 的值写出 P_m, 人们便会立刻注意到 R_m 满足条件

$$R_m\left(\frac{1}{x}\right)=(-1)^{m+1}x^2R_m(x).$$

它是个容易由对 m 的归纳证实的关系. 因此或者以别的方式, 欧拉发现对于每个偶数 $m>0$ 有 $\varphi(-m)=R_m(1)=0$ (*Eu.*I-14,442 于 E130 中;1739).

当人们甚至只计算了 $\varphi(-m)$ 对奇的 $m\geq 1$ 前面几项时, 一个非常令人惊讶的结果出现了; 当欧拉做此事时, 他必定立刻就清楚知道这些值与 $\zeta(m+1)$ 的值有关系, 而对后者他曾逐个地发现了它们与伯努利数 b_{m+1} 有关. 实际上, 它们之间的关系可以写成为

$$\varphi(-m)=R_m(1)=(2^{m+1}-1)\frac{b_{m+1}}{m+1},$$

它对于所有奇数 $m>0$ 成立, 又因为上式两端对于偶数 $m>0$ 均为 0, 故上式对于所有偶数 $m>0$ 也成立. 1739 年, 在已经对 $m=1,3,5,7$ 计算后, 欧拉对此结果选取了下面的形式:

$$1-2^m+3^m-4^m+\cdots=\frac{\pm 2\cdot 1\cdot 2\cdot 3\cdot\ \cdots\ \cdot m}{\pi^{m+1}}\left(1+\frac{1}{3^{m+1}}+\frac{1}{5^{m+1}}+\cdots\right),$$

对于 $m = 1, 3, 5, 7$ 分别选交替的符号 $+, -, +, -$; 这里右端的级数明显地具有值 $(1 - 2^{-m-1})\zeta(m+1)$.

欧拉把这件事在这里一放就是十年, 一直到最终他找到了一个一般性的证明为止, 当然如他所说用了 "一个最奇特的方法" ["*Il faut employer une méthode toute particulière pour démontrer cette harmonie*":*Eu.*I-15,75 于 E352 中;1749]. 这个 "奇特的" 方法在于欧拉–麦克劳林公式对级数 $\varphi(-m)$ 的完全不讲道理的应用, 这是如此地在撞大运, 以致几乎没有办法在此描述它; 甚至欧拉, 如果不是有他掌握的两个检验在每个特殊情形下的结果的方法, 也会犹豫是否还要将其向前推进; 这两个方法之一已在前面指出过, 而另一个可参看 *Eu.*I-14,594–595 于 E247 中;1746, 以及 *Eu.* I-10,222–224, 于《*Institutiones Calculi Differentialis*》的第 I 章第 II 部分中. 不管怎样, 他确实得到了上面显示的那个正确的值, 从而证实了上述公式对于奇 $m > 0$ 的有效性.

然而这一次, 欧拉没有在此止步. 将 m 替换为 $n-1$, 并用函数 φ 重写这个结果, 得到了

$$\frac{\varphi(1-n)}{\varphi(n)} = -C_n \frac{1 \cdot 2 \cdot 3 \cdot \ \cdots \ \cdot (n-1) \cdot (2^n - 1)}{(2^{n-1} - 1)\pi^n},$$

其中 $C_n = (-1)^{n/2}$, 这对所有偶数的 $n > 0$ 成立. 欧拉看出其左端对所有奇数 $n > 1$ 取 0 值, 故而如果对这样的 n 令 $C_n = 0$, 那么这个公式对这样的 n 也成立.

从他早年在彼得堡的日子以来欧拉一直对于给定初始值为整数的函数和公式的插值问题感兴趣; 他就是用如此的办法创建了 Γ- 函数理论 (*Corr.*I,3–4;1729). 毫不奇怪, 他寻求对上面的公式做同样的事, 即将 C_n 替换成 $\cos \pi n/2$, $(n-1)!$ 替换成 Γ 函数, 即后来由勒让德引进记号的 $\Gamma(n)$. 其结果等价于我们所知道的 ζ 函数的函数方程. 根据欧拉所知的关于 Γ- 函数的知识, 它对于所有正负整数均成立 (包括 $n = 0$ 和 $n = 1$), 也对 $n = \frac{1}{2}$ 成立, 而且可在他计算的精确范围内对于其他的 n 值进行数值的检验. 他给他的文章起了个适当的标题 "*Remarques sur un beau rapport entre les séries de puissances tant directes que réciproques*" (论幂级数之间正反两方面的漂亮关系: *Eu.*I-15,70–90=E352;1749). 此外他还加进了用同样方法得到的对于函数

$$L(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots$$

的函数方程. 他写道, "这最后的猜想是用一个比前面那个更简单的公式表达的; 由于它同样是可靠的, 故希望寻找对它的一个完全证明的努力将很可能取得成功; 这也必定会使许多相似的研究变得清晰起来" ["*Cette dernière conjecture renferme une expression plus simple que la précédente; donc, puisqu'elle est également*

certaine, il y a à espére qu'on travaillera avec plus de succés à en chercher une démonstration parfaite, qui ne manquera pas de répandre beaucoup de lumière sur quantité d'autres rechereches de celle nature": *Eu*.I-15,90].

欧拉写于 1749 年的文章出现在 1768 年柏林科学院的学术论文集中; 从未重印过. 曾出现在欧拉 1739 年文集 (E130, 只在 1750 年的彼得堡《*Commentarii*》中发表过) 中的一些结论, 以远没有什么启发性的形式在 1773 年又被重复, 并冠以不怎么样的标题 ("分析习题集 (*Exercitationes Analyticae*)": *Eu*.I-15,131–167=E432;1772). 在它们被发现后的一百年中, 欧拉的函数方程彻底被遗忘了. 甚至在 1849 年, 当 Schlömilch和 Malmstén 提及 $L(s)$ 的函数方程时, 他们两人都明显只是出于好奇. 1859 年黎曼复活了这个课题; 它的更进一步的历史与我们这里无关.

§3.21 数的分拆 (*Partitio numerorum*) 与模函数

1740 年 9 月正当欧拉已经在考虑迁居到柏林的事时 (参看 *Corr*.II,461;1740), 他收到从他未来的同事 P. Naudé的一封信, 信中提出了许多数学问题 (*Eu*.IV A-1,no.1903; 1740 年 8 月 29 日).

Naudé 是位新教的法裔数学家, 他那时在柏林很活跃并于 1745 年逝世在这里, 享年仅 61 岁. 在那时他写信给欧拉问问题是件自然的事; 他问了关于欧拉对级数 $\zeta(2n)$ 求和的细节. 另一个问题涉及佩尔方程. 最后 Naudé 提出了一个组合问题: 对于一个给定的数 m 有多少种方式将其分拆成 μ 个 (正) 整数之和, 并且所有这些分拆互不相同? 它可以分拆成多少种 μ 个 (正) 整数之和, 这些整数可以相同也可不同? 譬如对于 $m = 50$, $\mu = 7$ 的答案是什么?

欧拉在 9 月 23 日以 "新方式" 回答了 Naudé(*PkU*. 193–205, "老方式" 的日期为 1740 年 9 月 12 日). 那时在柏林与彼得堡之间的信件正常地要不少于 10 到 12 天来传递; 所以欧拉的答复相当迅速, 尽管他也为他的缓慢而道过歉 (他写道:" 由于我不好的视力使我遭受了几个星期的折磨":*PkU*.193; 参看 *Corr*.I,102;1740, 以及前面的 §3). 但是他不仅能够给出关于 $\zeta(2n)$ 的全面的细节, 而且他已经可以大体描述出 Naudé 最后一个问题的解, 从而实际上开创了分析的一个新的分支, 他称其为 "*Partitio Numerorum*". 不久在他亲自提交给彼得堡科学院一份研究报告中给出了对他的结果的完整阐述, 这是他离开彼得堡到柏林前的最后一份研究报告 (*Eu*.I-2,163–193=E158;1741 年 4 月 6 日). 他在他的《无穷分析导论》的第 XVI 章中 (*Eu*.I-8,313–338) 以及一篇在柏林写的文章中 (*Eu*.I-2,254–294=E191;1750) 更加详细地阐述了这个课题, 后来又在彼得堡写了一篇文章, 补充了更多的一些结果 (*Eu*.I-3,131–147=E394;1768).

像他立即感受到的那样 (甚至可能在他从 Naudé那里知道之前: 参看 *PkU.* 203), 这种问题的关键在于考虑一个或多个不定元的适当的形式幂级数, 以及在二项式的乘积 (有限或无穷) 与它们展开为和或级数的展式之间的关系; 至于后一个方面, 他也在他对三角函数的研究中以及在关于 "欧拉乘积" 中遇到过 (参见上文 §18–§19). 现在为了解决 Naudé 的问题, 他首先引进了无穷乘积 $\prod_i(1+x^iz)$; 使用现代了的记号, 他的计算如下. 令

$$P(x,z)=\prod_{i=1}^{\infty}(1+x^iz)=\sum_{\mu=0}^{\infty}Z_\mu(x)z^\mu=\sum_{m,\mu=0}^{\infty}N_{m,\mu}x^mz^\mu;$$

他看出 $N_{m,\mu}$ 是 m 可以表达为 μ 个不同整数和的方式的个数, 即出现在 Naudé的第一个问题中的那个数. 我们现在有

$$P(x,z)=(1+xz)P(x,xz),$$

于是使两端恒等, 有

$$A_\mu(x)=A_\mu(x)x^\mu+A_{\mu-1}x^\mu.$$

对 μ 进行归纳, 给出了

$$A_\mu(x)=\frac{x^{\mu(\mu+1)/2}}{(1-x)(1-x^2)\cdots(1-x^\mu)}.$$

现在令

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^\mu)}=\prod_{i=1}^{\mu}(1+x^i+x^{2i}+\cdots)=\sum_{m=0}^{\infty}M_{m,\mu}x^m;$$

$M_{m,\mu}$ 是 m 可以表达为属于集合 $\{1,2,\cdots,\mu\}$ 中 (任意多个) 整数之和的方式的个数. 这给出了

$$A_\mu(x)=x^{\mu(\mu+1)/2}\sum_{m=0}^{\infty}M_{m,\mu}x^m,\quad N_{m,\mu}=M_{m-\mu(\mu+1)/2,\,\mu}.$$

另一方面, 欧拉也引进了乘积

$$\begin{aligned}Q(x,z)&=\prod_{i=1}^{\infty}(1-x^iz)^{-1}=\prod_{i=1}^{\infty}(1+x^iz+x^{2i}z^2+\cdots)\\&=\prod_{\mu=0}^{\infty}B_\mu(x)z^\mu=\prod_{m,\mu=0}^{\infty}N'_{m,\mu=0}x^mz^\mu;\end{aligned}$$

这里的 $N'_{m,\mu}$ 是 Naudé的第二个问题中的数, 即 m 可写成不管是否相同的 μ 个整数和的方式的个数. 这里有

$$Q(x, xz) = (1 - xz)Q(x, z),$$

从而如上面那样进行便得到

$$B_\mu(x) = \frac{x^\mu}{(1-x)(1-x^2)\cdots(1-x^\mu)}, \quad N'_{m,\mu} = M_{m-\mu,\mu}.$$

从这些事实欧拉便能推导出在系数 $M_{m,\mu}$ 之间的许多递归公式, 并能够构造出对这些数的一个大范围的表. 涉及分拆的另一个值得注意的恒等式是下面的

$$\prod_{i=1}^{\infty}(1+x^i) = \frac{\prod_{i=1}^{\infty}(1-x^{2i})}{\prod_{i=1}^{\infty}(1-x^i)} = \frac{1}{\prod_{i=1}^{\infty}(1-x^{2i-1})},$$

由上面同样的论证知, 它将一个整数表成不同整数和的方式的个数与把它表示成不管相同与否的奇整数之和的方式的个数联系了起来.

当然欧拉立刻便明白, 他的数 $M_{m,\mu}$ 当 μ 增加时具有 "稳定" 性; 更准确地说, 它们对于 $\mu \geq m$ 与 μ 无关, 从而有

$$\prod_{i=1}^{\infty}(1-x^i)^{-1} = \sum_{m=1}^{\infty} M_{m,m}x^m.$$

在 1741 年这已经提示他计算乘积 $\prod_{i=1}^{\infty}(1-x^i)$ 了. 他写道: "让我以一个值得注意的观察来结束本文吧, 而对它我还不能以几何的严谨给予证明" ["*Finem huic dissertationi faciat observatio notatu digna, quam quidem rigore geometrico demonstrare mihi nondum licuit*": *Eu.*I-2,191 于 E158 中;1741]. 按照欧拉的猜想的结果算到不少于 51 个因子, 有:

$$\begin{aligned}&(1-x)(1-x^2)\cdots(1-x^{51})\\ &= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + \cdots,\end{aligned}$$

这实在令人吃惊; 在这个级数中, 所有的系数均为 0 或者 ± 1, 对于指数欧拉立刻认出是对于 $n = 0, -1, +1, \cdots, -5, +5, -6$ 的 "五角数" $\frac{1}{2}n(3n+1)$, 这提示了著名的公式

$$\prod_{i=1}^{\infty}(1-x^i) = \sum_{n=-\infty}^{+\infty}(-1)^n x^{n(3n+1)/2}$$

(*Eu.*I-2,191–192 于 E158 中;1741; 参看 *Corr.*II,467–468;1741 年 1 月 28 日, *Eu.*I-2,280–281 于 E191 中;1750 以及《无穷分析导论》第 XVI 章的 *Eu.*I-8,332). 它及

其推广在下一个世纪的 1829 年雅可比的《*Fundamenta Nova*》中以及他后来关于 θ- 函数的全部工作中起了中心的作用 (参看 *Jac.*I,234–236, 以及 *Eu.*I-2,191–192, 注 1). 当然欧拉的先知天赋并没有到此为止, 对他而言这个公式只不过是个相当于一个算术结果的形式恒等式罢了.

一些年后他将此公式转变为关于算术函数的一个陈述, 他以 $\int n$ 表示这个函数 (参看前面的 §6); 它是包括 1 和 n 的所有因子的和, 现在我们一般把它写为 $\sigma_1(n)$; 他对它的兴趣是由于后来处理 "亲和数" 引起来的 (*Eu.*I-2,59–61=E100;1747, *Eu.*I-2,86–162=E152;1747). 取乘积 $\prod(1-x^i)$ 的对数导数, 则形式地得到

$$\frac{d}{dx}\log\prod_{i=1}^{\infty}(1-x^i) = -\sum_{i=1}^{\infty}\frac{ix^{i-1}}{1-x^i}$$
$$= -\sum_{i=1}^{\infty}\left(i\sum_{\nu=1}^{\infty}x^{\nu i-1}\right) = -\sum_{N=1}^{\infty}\left(\int N\right)x^{N-1};$$

将此与欧拉恒等式中级数的对数导数相等, 得到

$$\sum_{n=-\infty}^{+\infty}(-1)^n\int\left(N-\frac{1}{2}n\Big(3n+1\Big)\right)=0,$$

其中我们假定了对于所有 $m<0$ 有 $\int m=0$, 并假定如果 $\int 0$ 出现在此关系中, 则将其换作 N, 即如果 N 等于 "五角数" $\frac{1}{2}n(3n+1)$. 欧拉一点也没有浪费时间, 马上把它递给了哥德巴赫, 称其为 "*eine sehr wunderbare Ordnung* (一个非常美妙的规则)" (*Corr.*I,407–408;1747 年 4 月 1 日); 他非常快地将它写了出来并在下面标题下发表: "*Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs*(关于数的因子和的一个非常特别规则的发现)" (*Eu.*I-2,241–253=E175;1747 年 6 月 22 日). 他还不怀疑它的有效性: "*elle appartient à ce genre dont nous pouvons nous assurer de la vérité, sans en donner une démonstration parfaite*"[" 它属于那样一类结果, 它的真实性即便我们还不能给出一个完善的证明也是确定的": *Eu.*I-2,242].

当然这并没有让他停止寻找一个 "完善的证明", 而 (当然, 要是很想说的话) 他找到了一个 (*Corr.*I,522–524;1750; *Eu.*I-2,390–398=E244;1751). 这个证明是代数精湛技巧的炫目展示然而却相当初等, 有赖于一系列形式幂级数的构造, 它们是 $P_0=\prod(1-x^n)$, P_1, P_2 等, 使得对于所有的 $n>0$ 成立如下关系:

$$P_{n-1}=1-x^{2n-1}-x^{3n-1}P_n,$$
$$P_n=\sum_{\nu=0}^{\infty}x^{\nu n}(1-x^n)(1-x^{n+1})\cdots(1-x^{n+\nu}).$$

$n=1$ 的情形由显然的恒等式

$$\prod_{n=1}^{\infty}(1-\alpha_n)=1-\sum_{n=1}^{\infty}\alpha_n(1-\alpha_1)(1-\alpha_2)\cdots(1-\alpha_{n-1})$$

对乘积 $\prod(1-x^n)$ 的直接应用得到. 假定对 P_i 已经能够找到了 P_n, 我们于是有

$$P_n=1+x^n(1-x^{n+1})+\sum_{\nu=2}^{\infty}x^{\nu n}(1-x^{n+1})\cdots(1-x^{n+\nu})$$
$$-x^n-\sum_{\nu=1}^{\infty}x^{\nu n+n}(1-x^{n+1})\cdots(1-x^{n+\nu}).$$

在前面有一个和号中将 ν 换成 $\nu+2$, 而在后一个中换成 $\nu+1$, 那么将这两个结合起来则发现这的确正好是 $1-x^{2n+1}-x^{3n+2}P_{n+1}$, 故可对 n 进行归纳. 这对于所有 $n>0$ 给出了

$$P_0=1-x-x^2(1-x^3)+x^{2+5}(1-x^5)-\cdots+(-1)^n x^{2+5+\cdots+(3n-1)}P_n,$$

从而完成了证明.

欧拉在用同一背景下产生的另一个闪光的思想方面则没有那么成功. 在开始将费马关于 “三个三角数, 四个平方数, 五个五角数等” 的断言合理地看成是属于 “*partitio numerorum*” 这个课题后, 他自然想到将形式幂级数的方法应用到它, 这个方法曾是他为上述目的而引进的 (*Corr.*I,531–532;1750; 参看 *Eu.*I-3,132,144–145 于 E394 中;1768). 譬如, 他看出四平方数的断言等于是说, 如果将 s 写成形式幂级数

$$s=1+x^1+x^4+x^9+\cdots,$$

于是 x 的所有的幂全在级数 s^4 中以非零系数出现; 当然他充分了解 x^n 在 s^4 中的系数表示了有多少个方式将 n 写成四个平方数. 他对哥德巴赫写道, “这对我来说这是达到对费马定理证明的最自然的方式” [“*Dieser Weg däucht mir noch der natürlichste zu seyn, um zum Beweis der theorematum Fermatianorum zu gelangen*”: *Corr.*I,532;1750]. 除了将 s 替换为 “θ 级数”

$$2s-1=\sum_{n=-\infty}^{+\infty}x^{n^2}$$

外, 我们所讨论的这个定理, 正是雅可比在他的《*Fundamenta*》中证明的值得称赞的结论, 因此实现了欧拉的预言. 欧拉并不满足于仅仅将 s 考虑为一个幂级数; 如果他不去找进行数值计算的场合, 这就不是欧拉他自己了; 吸引他的是当 x 趋向于 -1 时它的性态, 或者完全相同的, 级数

$$t=1-x^4+x^9-x^{16}+\cdots$$

在 $x=1$ 附近的性态 (*Corr.*I,529–531;1750). 这里, 首先将 x 替换为 $1-y$, 我们形式地得到

$$\sum_{n=0}^{\infty}(-1)^n(1-y)^{n^2}=\frac{1}{2}+0\cdot y+0\cdot y^2+0\cdot y^3+\cdots,$$

这是他早期的结果的一个容易的推论, 按照这个早期结果, $1^m-2^m+3^m-\cdots$, 对于偶数 $m>0$ 为 0, 对于 $m=0$ 为 $\frac{1}{2}$ (参看前面的 §20). 他暗示我们当 x 趋向 1 时, $2t-1$ 趋向 0 的速度要比 $1-x$ 的任何幂的要快, 这是欧拉寻求证实的一个预想结果, 他对 $x=0,\frac{1}{2},\frac{2}{3},\frac{7}{10},\frac{9}{10}$ 逐次地对 t 计算到 10 位小数 (由于级数 t 在 x 靠近 1 时的慢收敛性, 这没有什么建树). 他写信给哥德巴赫说:" 但是我白白地寻找了对于 $x=1-\omega$ 当 ω 非常小时从数值上求此级数和的可信办法, 这个办法对于做这些问题会有很高的价值" [*"es wäre eine Methode hoch zu schätzen, vermittellelst welcher man im Stande wäre den Werth von t proxime bestimmen, wenn ω ein sehr kleiner Bruch ist"*:*Corr.* I,531]. 在这里人们必定再一次钦佩欧拉判断的可靠性; 对他的问题的答案包含在了 θ 级数的函数方程中; 雅可比在他的《*Fundamenta*》中也将它呈献给了数学世界.

§3.22 结论

欧拉的算术工作, 虽说延伸了五十多年, 但也只构成了他的数量巨大的成品中的一小部分. 然而他的科学气质的主要特征从上面的概述中已显露了出来.

或许这个气质的最突出的特色是非凡的机敏 (promptness), 由于这种机敏他甚至对于不经意的提示或者刺激都有反应: 一个从哥德巴赫来的关于费马数 $2^{2^n}+1$ 的素性问题 (参看前面的 §4,§5(a) 以及 §6); 一个他开始甚至也没有完整地读过的费马关于四平方数之和的陈述 (同上,§4,§5(b),§11); 一个由 Naudé 提出的初等组合问题 (§5(h),§21); 在一本由罕为人知的意大利贵族写的书中几个孤立的定理 (§5(e),§15); 拉格朗日关于模素数的同余定理 (§6); 拉格朗日对于费马四平方和的多少有点不太恰当的证明 (§11) 等等. 他也没有忽视观察的机会, 诸如他对 $\prod(1-x^n)$ 的计算 (参看 §21); 在收到法尼亚诺的书 (索引同上, §15) 后他曾写道:"这样的观察更加有价值". 每个机会都被迅速地抓住了; 每一个都为他的磨坊提供了谷物, 常常引起一长串令人印象深刻的研究.

令人同样印象深刻的是, 一旦一个问题引起了欧拉的永不满足的好奇心他就从不放弃. 其他的数学家, 譬如希尔伯特, 将他们的生活清楚地分成不同的时期, 在每个时期致力于一个单独的课题. 欧拉不是这样. 穷其一生, 即便在丧失视力之后, 似乎在他脑袋里装着他那个时代的整个数学, 不管是纯粹的还是应用的. 一旦他开始着手一个问题, 不仅他会一次又一次地回到它, 很少关心是否

有时他只是在重复自己, 而且他喜爱把他的网撒得越来越宽而永不丧失热情, 总是期望揭开越来越多的秘密, 越来越多的正徘徊在下一个角落周围的 "*herrliche proprietates*(辉煌的性质)". 不管是他还是其他人做出了这个发现对他来说都无大关系. 在知道拉格朗日对他自己关于椭圆积分工作的补充后, 他写道 :"*Penitus obstupui*" ("使我大吃一惊": *Eu.*I-21,1 于 E506 中;1777; 参看他给拉格朗日的信, *Eu.*IV A-5,505;1775); 之后他对拉格朗日的成果进行了改进. 甚至当一个问题已经解决得使他满意时 (如发生在他对费马定理 $a^p \equiv a \mod p$ 的第一个证明, 或者在 1749 年关于两个平方数和的第一个证明) 他从来没有停下他追求更好的证明, "更自然的" (*Eu.*I-2,510 于 E262 中;1755; 参看 §6), "容易的" (*Eu.*I-3,504 于 E552 中;1772; 参看 §6), "直接的" 证明 (*Eu.*I-2,365 于 E242 中;1751; 参看§6); 并且反复发现它们.

一些问题整个一生都与他失之交臂. 其中最突出的, 就涉及数论而言, 或许是他对于二次互反律的一些猜想, 这些猜想形成于 1742 年或其后不久, 并且他直到生命的最后仍旧在强调它的重要性 (参看 §5(i),§8,§9); 那时他很少能有望得到他自己的一个证明但他表达了他有信心的期盼: 它们的证明就会 "很快出现" ["*quam...mox expectare licebit*":*Eu.*I-4,191 于 E598 中;1775]. 哪怕他能看到 1785 年勒让德给出的部分证明, 更不要说高斯在 1796 年所发现并在 1801 年发表的完全证明了, 他会多么的快乐啊! 它没有让他到达期望的乐土; 但他的双眼现在转向了内心, 让他瞥见了它的光彩, 或者用他自己的话说, 它的 *Herrlichkeit* (辉煌).

附录 I 二次互反律

我们在前面的 §8 曾解释过 (参看第二章 §12), 一个为奇数并且不是 N 的因子的素数 p 是在欧拉意义下的一个 "形式 X^2+NY^2 的素因子" 是说, 如果它除尽某个整数 a^2+Nb^2, 其中 a 与 Nb 互素, 这等价于说, 或者 $-N$ 是一个模 p 的二次剩余, 或者另一种说法, p 在域 $\mathbb{Q}(\sqrt{-N})$ 中分解出两个素理想因子. 我们在这里的目的是要描述关于那些具有最适合于与欧拉的实验式的结果相比较的那些素数.

不失一般性, 我们将假定 N 无平方因子, 且既非 0 也非 -1; 我们将按照 $N \equiv -1 \pmod 4$ 与否而令 $d=-N$ 或 $d=-4N$, 并令 $D=|d|$. 于是有一个整数的函数 ω, 满足如下性质:

(I) *如果 n 与 D 互素, 则 $\omega(n) \equiv \pm 1$, 否则 $\omega = 0$.*

(II) *ω 是以 D 为周期的周期函数*, 即对于所有 n,

$$\omega(n)=\omega(n+D);$$

这也可以表达为, ω 是个模 D 的整数的函数.

(III) 对所有的 m 和 n 有 $\omega(mn)=\omega(m)\omega(n)$. 这可表达为 ω 是模 D 的一个"狄利克雷特征标". 特别地, 对于所有与 D 互素的 n 有 $\omega(n^2)=1$.

(IV) 按照 N 为 <0 还是 >0 决定 $\omega(-1)$ 为 $+1$ 还是 -1.

(V) 没有除 D 自己以外的 D 的因子 D' 使得只要 m, n 与 D 互素且 $m\equiv n \pmod{D'}$, 就有 $\omega(m)=\omega(n)$. 这可表达为, ω 是模 D 的本原特征标; 根据 (I) 和 (III), 它等于是说不存在 D 的不同于自己的因子 D', 使得只要 n 与 D 互素且 $\equiv 1 \pmod{D'}$ 就有 $\omega(n)=1$.

最后, ω 与 X^2+NY^2 的素因子问题的相关性由下面给出:

(VI) 一个奇素数 p 是 X^2+NY^2 的素因子当且仅当 $\omega(p)=+1$.

根据 (I),(II) 和 (III), ω 决定了一个乘群 $G_D=(\mathbb{Z}/D\mathbb{Z})^{\times}$, 即模 D 的与 D 互素的整数群上的二阶特征标 (在现在通常群论的意义下的); 因此它的核, 即那些在它上取 1 的模 D 同余类的集合, 是 G_D 的一个指数为 2 的子群; 按照 (III), 这个核包含了模 D 的二次剩余 G_D^2.

现在要证明条件 (I) 到 (V) 决定了这样一个函数 ω, 而且唯一决定了它. 首先讨论 D 为素数的情形; 即只要 $N=\pm q$, q 为奇素数而符号由 $N\equiv -1 \pmod 4$ 决定便是这种情形. 对于这种情形, 欧拉在不迟于 1751 年便发现了 (*Eu.*I-2,339–355 于 E242 中;1751; 参看《*Tractatus*》, *Eu.*I-5,227–230 的 no.284–307, 以及前面的 §6) 二次剩余构成了 $G_D=G_q$ 的一个指数 2 的子群. 因此 $\omega(n)$ 根据 n 是模 q 的二次剩余还是非二次剩余决定是 $+1$ 还是 -1; 使用从勒让德以来一直使用的记号 (参看第四章,§6) 就是 $\left(\frac{n}{q}\right)$, 或者紧缩为 (n/q). 满足 (IV) 只不过是决定 -1 模 q 的二次剩余 $(-1/q)$, 这是由欧拉在 1749 年得到的 (参看前面的 §6, 以及第二章 §7).

在一般情形, 写出 $D=q_0q_1q_2\cdots q_r$, 其中 q_0 为 1, 4, 或 8, 而 q_1, $q_2,\cdots,q_r$ 为不同的奇素数. 欧拉知道, 至少在写《*Tractatus*》那个时候以来就知道, 一个整数为模 D 二次剩余当且仅当它对模每一个 q_i 为二次剩余. 用现代的说法, $G_D/(G_D)^2$ 为 $(2,2,\cdots,2)$ 型, 分别按照 q_0 为 1,4,8 而有 2^r, 2^{r+1}, 2^{r+2} 个元素; 它的每个特征标可写成 (n/q_i), $i=1,2,\cdots,r$ 以及当 $q_0=4$ 或 8 时的模 q_0 的特征标中的全部或部分的乘积; 一个诸如 ω 的本原特征标对于与 D 互素的 n 必定由乘积

$$\omega(n)=\psi(n)\prod_{i=1}^{r}\left(\frac{1}{q_i}\right)$$

给出, 其中如果 $q_0=1$, 则 $\psi=1$, 否则 ψ 是个模 q_0 的本原特征标. 如果 $q_0=4$, 则只有一个这样的特征标 ψ_0 由 $\psi_0(1)=1,\psi_0(-1)=-1$ 给出. 如果 $q_0=8$ 我们则有 $G_8=\{\pm1,\pm3 \mod 8\}$; G_8 的一个本原特征标必定满足 $\psi(-3)=-1$, 这是

因为否则的话, $\psi(n)$ 会只依赖于 n 模 4 的值; 因此只有两个这样特征标 ψ_1, ψ_2, 它们分别由 $\psi_1(-1)=1$, $\psi_2(-1)=-1$ 决定. 如果 $q_0=8$, 出现在上面关于 ω 的公式中的特征标 ψ 因而是由条件 (IV) 决定的那个, 即由

$$\psi(-1)=\operatorname{sgn}(-N)\prod_{i=1}^{r}\left(\frac{-1}{q_i}\right)$$

给出, 其中 $\operatorname{sgn}(-N)$ 根据 $-N>0$ 还是 <0 决定为 1 还是 -1. 当 ω 如上那样决定时, 那么对 $q_0=1$ 或者 4 也满足条件 (IV) 是由对任意一个奇素数 q 确定 $(-1/q)$ 这个事实的又一次的简单推论.

至于条件 (VI), 它现在可写成

$$\left(\frac{-N}{p}\right)=\omega(p)$$

(这对所有不除尽 N 的奇素数都满足), 先讨论 $N=1$ 的情形. 于是 $D=4$; ω 是模 4 特征标 ψ_0; 从而 (VI) 说的是 $(-1/p)=\psi_0(p)$, 这的确就是这个情形. 让 $N=\pm2$; 于是 $D=8$; ω 当 $N=-2$ 时为 ψ_1, $N=+2$ 时为 ψ_2 ; 于是 (VI) 说的是 $(2/p)=\psi_1(p)$, $(-2/p)=\psi_2(p)$, 这就是我们在 §9 中所知道的情形.

现在让 $N=\pm q$, 其中符号由 $N\equiv-1 \pmod 4$ 决定, 故而 $D=q$. 于是 (VI) 可以写成

$$\left(\frac{\mp q}{p}\right)=\left(\frac{p}{q}\right),$$

其中 p, q 为两个不同的奇素数, 而符号是使得 $\mp q\equiv 1 \pmod 4$. 由于先决定了 $(-1/p)$, 这等于是勒让德在 1785 年第一次所阐述的二次互反律[7](参看下文的第四章§6). 因此上述 ω 的性质 (I) 到 (VI) 可以说是包含了二次互反律. 现在, 假定它成立, 我们将证明条件 (VI) 对所有 N 的值都满足.

再次如前面那样, 令 $D=q_0q_1\cdots q_r$, 并且对于 $i=1,2,\cdots,r$ 令 $q_i'=\pm q_i$, 其符号由 $q_i'\equiv 1 \pmod 4$ 决定. 我们可以写成 $-N=q_0'q_1'\cdots q_r'$, 其中 $q_0'=\pm1$ 或者 ±2. 于是有

$$\left(\frac{-N}{p}\right)=\left(\frac{q_0'}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i'}{p}\right)=\left(\frac{q_0'}{p}\right)\prod_{i=1}^{r}\left(\frac{p}{q_i}\right).$$

在上面我们已注意到有 $(q_0'/p)=\psi'(p)$, 其中的 ψ' 按照 q_0' 为 $+1$, -1, $+2$, -2 分别为 1, ψ_0, ψ_1, ψ_2; 如果我们能证明 ψ' 与出现在 ω 的定义中的特征标 ψ 是

[7]对此课题最清晰的阐述是在狄利克雷的《*Vorlesungen über Zalentheorie*》(ed. R. Dedekind, Braunschweig 1894) 中. 或许关于所讨论的这个 "互反律" 已知的最简单证明是艾森斯坦的, 参看 A. 韦伊的《*Number Theory for Beginners*》, Springer,1979,§XII. 也可参看 J.-P. 塞尔的《*Couurs d' Arithmétique*》, P.U.F.,Paris 1970, 第一章 (有中译本).

一样的, 那么这个证明便完成了. 对于 $q_0' = 1$ 情形确实如此, 这是因为这时我们有 $-N \equiv 1 \pmod 4$, $D = |N|$, $q_0 = 1$, $\psi = 1$. 相似地, 如果 $q_0' = -1$, 我们有 $N \equiv 1 \pmod 4$, $D = 4|N|$, $q_0 = 4$, $\psi = \psi_0$. 现在考虑情形 $q_0' = \pm 2$; 于是 $D = 4|N|$, $q_0 = 8$, $\psi = \psi_1$, 或者 ψ_2, 从而我们必须证明 $\psi(-1) = \psi'(-1)$. 但是这时我们有

$$\operatorname{sgn}(q_i') = \left(\frac{-1}{q_i}\right), \ \operatorname{sgn}(-N) = \operatorname{sgn}(q_0') \prod_{i=1}^{r} \left(\frac{-1}{q_i}\right),$$

从而

$$\psi(-1) = \operatorname{sgn}(q_0') = \psi'(-1),$$

这便完成了我们的证明.

最后, 为了便于将上面的结果与欧拉的猜想 (参看 §8) 进行比较, 合适的办法是, 引进由 ω 在模 $4|N|$ 的乘群上诱导的特征标的核 K_N, 即 ω 在其上取值 1 的模 $4|N|$ 且与 $4|N|$ 互素的同余类的集合. 这明显具有如下的性质:

(A) K_N 是模 $4|N|$ 乘群的指数为 2 的子群.

(B) -1 是否属于 K_N 依赖于 $N<0$ 或 $N>0$.

(C) 如果 r 和 s 与 $4|N|$ 互素并且如果 $r \equiv s \pmod D$, 则只要它们其中一个属于 K_N, 那么两者都属于, 并且 D 的任何不同于 D 的因子 D' 都不具有此性质.

反之设 K_N 为模 $4|N|$ 乘群的一个指数为 2 的子群, 它满足 (B) 和 (C). 设 ω' 为模 $4|N|$ 的整数上的函数, 使得当 n 与 $4|N|$ 不互素时有 $\omega'(n) = 0$, 而当 n 属于 K_N 时有 $\omega'(n) = 1$, 又当 n 与 $4|N|$ 互素且不属于 K_N 时有 $\omega'(n) = -1$. 对于 $N \equiv 1$ 或者 $2 \pmod 4$, ω' 满足上面列出的从 (I) 到 (V) 的所有条件, 故而它就是 ω. 现在取 $N \equiv -1 \pmod 4$, 故而 $D = |N|$. 定义整数上的函数 ω'' 为: 当 n 与 N 不互素时 $\omega''(n) = 0$, 当 n 与 N 互素, r 与 $4|N|$ 互素且 $n \equiv r \pmod{|N|}$ 时 $\omega''(n) = \omega'(r)$; 根据 (C), 这与 r 的选取无关, 故而 ω'' 确有定义; 容易看出, ω'' 满足从 (I) 到 (V) 的所有条件, 故而它与 ω 相同. 这表明在前一种情形里的 ω' 和在后一种情形的 ω'' 满足条件 (VI). 因此一个非 N 因子的奇素数是形式 $X^2 + NY^2$ 的一个因子当且仅当它属于模 $4|N|$ 的 K_N, 它正是欧拉在 1744 年所猜想的.

附录 II 对平方和问题的一个初等证明

1751 年, 欧拉在证明每个整数都是 (最多) 四个 “*in fractis*” 即有理数的平方和之后, 写下了下面的话:

"*In Analysi quidem Diophantea pro certo assumi solet nullum numerum integrum in quatuor quadrata fracta dispertiri posse, nisi eius resolutio in quatuor quadrata integra vel pauciora constet... Verum nusquam adhuc eiusmodi demonstrationem inveni...*" ["在丢番图分析中人们通常想当然地认为, 除非任意整数有四个或更少的整数平方和的表达式, 否则没有整数可以分解成四个有理数的平方,…… 但是至今我没在任何地方找到对此的证明……":*Eu.*I-2,372 于 E242 中;1751]. 对于《丢番图》的读者而言, 涉及 2, 3 或 4 个平方数和的确是个自然发生的问题, 并且费马在他作为数论学家的初期也已经给了他一些想法, 它们明显是不成功的 (参看第二章 §5). 欧拉自己也提出过它, 更特别地关注两个平方数和的问题, 而在 1745 年 (参看 *Corr.*I,312), 并一再重复地在给哥德巴赫的信中关注到四个平方数之和的问题 (参看 *Corr.*I,521;1750,527;1750,559;1751).

在这里我们将重新给出属于 L.Aubry 的一个证明 (*Sphinx-Œdipe* 7 (1912), pp.81–84), 它同样可适合用于 2, 3, 或 4 平方数和以及几个其他的二次型. 我们首先用几何的语言对于 3 个平方数和进行描述.

在 $\mathbb{R}^3$ 中的点被称为有理的 (分别地, 整的) 是说, 如果他们具有有理的 (分别地, 整的) 坐标. 对每个点 $a=(x,y,z)$ 有一个整点 $a'=(x;,y',z')$, 它离 a 的距离小于 1; 譬如可以取 x', y', z' 分别为最靠近 x, y, z 的整数, 这时从 a 到 a' 的距离 $\leq \sqrt{3}/2$.

现在假定一个整数 N 是三个有理数的平方和; 这等于是说在由 $N=x^2+y^2+z^2$ 给出的球面 S 上有一个有理点 a_0. 设 a'_0 为最靠近 a_0 的一个整点 (如果有两个以上的则选其中一个); 它与 a_0 的距离 <1. 称联结 a_0 与 a'_0 的直线交 S 的第二个点为 a_1; 它是个有理点. 设 a'_1 为最靠近 a_1 的整点; 设 a_2 为 a_1 与 a'_1 的连线与 S 的第二个交点; 等等. 现在要证明, 对于某个 n , a_n 是个整点.

令 $a_0=(x,y,z)$; 假定它不是个整点, 又令 m 为 x, y, z 的最小公分母; 记 $x=n/m$, $y=p/m$, $z=q/m$; 我们有

$$Nm^2=n^2+p^2+q^2.$$

令 $a'_0=(n',p',q')$ 为最靠近 a_0 的整点, 并令

$$r=n-mn', \quad s=p-mp', \quad t=q-mq',$$
$$N'=n'^2+p'^2+q'^2, \qquad M=2(nn'+pp'+qq').$$

a_0 与 a'_0 间的距离平方于是为

$$\frac{1}{m^2}(r^2+s^2+t^2)=N+N'-\frac{M}{m},$$

它可以写成 m'/m, 其中 m' 为整数; 因为它 <1, 我们有 $0<m'<m$, 并同时有

$$r^2+s^2+t^2=mm', \qquad M=m(N+N')-m'.$$

现在联结 a_0 与 a_0' 的直线由点

$$(n' + \lambda r, p' + \lambda s, q' + \lambda t)$$

组成; 在这里, 点 a_1 由方程

$$\begin{aligned} 0 &= (n' + \lambda r)^2 + (p' + \lambda s)^2 + (q' + \lambda t)^2 - N \\ &= mm'\lambda^2 + (M - 2mN')\lambda + N' - N \\ &= (m\lambda - 1)(m'\lambda + N - N') \end{aligned}$$

给出. 根 $\lambda = 1/m$ 对应于点 a_0, 故而另一个根 $\lambda = (N' - N)/m'$ 对应了 a_1. 因此 m' 是 a_1 的坐标的公分母; 由于它 $< m$, 这表明对于点 a_0, a_1, $a_2, \cdots$ 的坐标的公分母形成一个正整数的递降序列, 这证明了我们的断言.

在这个证明中所用到的二次型

$$F(X, Y, Z) = X^2 + Y^2 + Z^2$$

只有如下的性质: 对于每个非整点 (x, y, z), 存在一个整点 (x', y', z') 使得

$$0 < |F(x - x', y - y', z - z')| < 1.$$

这同样能有效地用到, 譬如, 形式 X^2+Y^2, $X^2\pm2Y^2$, X^2-3Y^2 上. 现在用一种显然的方式将记号修改一下, 我们来指出这同一个证明可以应用到 $\mathbb{R}^n$ 中的二次型 $F(x)$, 它在所有的整向量 x 上取整数值并使得对于 $\mathbb{R}^n$ 的非整向量 x 存在一个整向量 x' 满足 $0 < |F(x-x')| \leq 1$; 譬如,X^2+3Y^2, $X^2+Y^2+2Z^2$, $X^2+Y^2+Z^2+T^2$ 都属于这种情形. 定义双线性形式 $B(x, y)$ 为

$$F(\lambda x + \mu y) = \lambda^2 F(x) + \lambda\mu B(x, y) + \mu^2 F(y).$$

像前面那样, 取一个有理点 a_0 使得 $F(a_0) = N$, 以及一个整点 a_0' 使得

$$0 < |F(a_0 - a_0')| \leq 1.$$

设 m 为使得 $n = ma_0$ 为整点的最小整数; 令 $a_0' = n'$, $r = n - mn'$, $N' = F(n')$, $M = B(n, n')$. 我们有

$$F(a_0 - a_0') = F(m^{-1}r) = F(m^{-1}n - n') = N + N' - \frac{M}{m};$$

将此写为 m'/m, 我们有 $0 < m' \leq m$, 其中 m' 是个整数.

联结 a_0 与 a_0' 的直线由点 $n'+\lambda r$ 组成，而它与超曲面 $F(x)=N$ 的交点 a_1 由

$$0=F(n'+\lambda r)-N=mm'\lambda^2+(M-2mN')\lambda+N'-N$$
$$=(m\lambda-1)(m'\lambda+N-N')$$

给出. 像前面那样, a_1 对应于根 $\lambda=(N'-N)/m'$, 故 $m'a_1$ 是个整点而 m' 是 a_1 的坐标的公分母; 然而我们现在必须考虑情形 $|m'|=m$, 即 $|F(m^{-1}r)|=1$. 取 F 为上面列出的三个形式之一, 我们则可假定取 a_0' 为坐标最靠近 a_0 的坐标的整点或其中的一个, 从而使得 $m^{-1}r$ 的坐标的绝对值均 $\leq \frac{1}{2}$; 于是, 如果 $F(m^{-1}r)$ 为 1, 则它们必定全为 $\pm\frac{1}{2}$, 从而 $2a_0$ 必为整点, 故 $m=2$. 在这种情形对于 a_0' 则有 2^n 种可能的选择, 而这个选择可以使得 $N-N'$ 为偶数; 由于与此同时 m' 必为 1 或者 2, 故 a_1 为整点.

上面的证明可以被欧拉容易地理解; 或许稍加努力也会被费马理解, 因为他的代数技巧终究离所需的水准要少一点. 它之所以这样晚才被发现, 或许是要作为对那些寻求对这个被想象成深奥结果的初等证明的人们的一种鼓励吧.

附录 III 椭圆曲线的加法定理

我们在此的目的是要提供给欧拉的椭圆函数理论一个适当的背景. 像在第二章, 附录 II 中那样, 设 Γ 是定义在特征 0 的基域上的一条代数曲线. Γ 上的一个微分被理解为一个表达式 $\omega=f\cdot dg$, 其中的 f, g 为 Γ 上的有理函数; 它可等同于 $f(dg/dx)dx$, 在这里我们可取 x 为 Γ 上的任意非常值的有理函数.

对于 Γ 上的每个点 M 可配上一个以 M 为单零点的有理函数 x; 于是可以用它作为在 M 的一个局部坐标, 并且 Γ 上的每个函数 f 可以在 M 的一个邻域里表示为一个洛朗级数 $f=\sum_{i=n}^{\infty}a_ix^i$; 如果 $a_n\neq 0$, n 是 f 在 M 的阶; 如果 f 在 M 有 n 重零点则它 >0 , 如果 f 在 M 有 $-n$ 重极点, 则 <0 . 我们记得, 在 Γ 上一个非常值函数 f 的零点个数等于它的极点的个数, 这里的个数算进了它们的重数; 如果该数是 N, 而且 Γ 上所有有理函数构成的域是域 $K(f)$ 的 N 次代数扩域, 其中的 $K(f)$ 是 f 的有理函数域, K 是基域.

设 M, x 如上; 于是每个 Γ 上的微分 ω 可以在 M 的邻域中表达为 $\omega=\sum_{i=n}^{\infty}a_ix^idx$; 如果 $a_n\neq 0$, $n>0$, 则说它在 M 有一个 n 重零点, 如果 $a_n\neq 0$, $n<0$, 则说它在 M 有一个 $-n$ 重极点. 称它在 M 为恰当的是指它可写成 $d(\sum_{j=m}^{\infty}b_jx^j)$; 在 M 为恰当的充要条件是 $a_{-1}=0$. 称一个微分为第一类的是说如果它没有极点; 称为第二类是说如果它处处为恰当; 其余的称为第三类.

从此往后我们取基域为复域 $\mathbb{C}$. 于是微分可以沿 Γ 上任意 (逐段可微的) 路径积分; 沿一条闭道的这样的积分称为一个周期.

首先设 Γ 的亏格为 0; 于是在 Γ 上有一个阶数为 1 的有理函数 $R(x) = P(x)/Q(x)$, 其中 P, Q 为多项式; Γ 可以等同于 (在 $\mathbb{C}$ 上的) "射影直线", 也被称之为 "黎曼球面", 即在其上添加了无穷远处的一点的复变量 x 的平面, 记无穷远点为 $x = \infty$. 在 Γ 上没有第一类微分; 如果 $\omega = R(x)dx$ 是 Γ 上的任一微分, 于是 (如欧拉在实质上所证明的那样, 参看前面的 §7 和 §15) 它的差一个常数而有确定定义的积分 $\int \omega$ 总可以由有理的和对数的函数来表达 (如果基域是实域, 则如欧拉一直了解的那样, 可由有理的、对数的以及反三角的函数表达). 这个积分本身是一个有理函数, 就是说, 可以写作 $\omega = dS(x)$, 其中 S 为有理函数当且仅当 ω 是第二类积分.

其次, 设 Γ 为任意代数曲线; 设 $\sum_1^N A_i$, $\sum_1^N B_j$ 为 Γ 上两个等价的除子 (参看第二章, 附录 II); 假定对所有的 i, j, $A_i \neq B_j$. 这表明在 Γ 上有一个有理函数 x, 其阶为 N, 并有 N 个零点 A_i 和 N 个极点 B_j (每个均算上它们的重数). 那么 Γ 可以等同于展开在 x 的 "黎曼球面" 上的 N-叶黎曼面, 而 Γ 上的有理函数域可以写为 $\mathbb{C}(x,y)$, 其中 y 是 Γ 上的一个函数, 它在 $\mathbb{C}(x)$ 上为 N 次代数元. 取 y 在 $\mathbb{C}(x)$ 上的不可约方程:

$$P(x,Y) = \sum_0^N F_i(x)Y^{N-i} = F_0(x)\prod_1^N (Y - y_i) = 0,$$

其中 F_i 为多项式, $y_1 = y$. 设 $\omega = R(x,y)dx$ 为 Γ 上的一个任意微分; 令

$$\eta = \sum_1^N R(x,y_i)dx.$$

这可写成 $S(x)dx$, 其中 S 是个有理函数; 它是在 "射影直线" 上的一个微分. 如果 ω 为第一类, 则它也是第一类, 从而为 0; 如果 ω 是第二类, 则它也是第二类. 现在在 x- 平面上取从 $x = 0$ 到 $x = \infty$ 的任一条路径 λ; 它在 Γ 上的逆像由 N 条分别从 A_i 到 B_i 的 Γ 上的路径 λ_i 组成 $(1 \leq i \leq N)$, 这里的点 A_i, B_i 经过适当的重新编号. 这时我们有

$$\int_\lambda \eta = \sum_1^N \int_{\lambda_i} \omega.$$

如果 ω 为第一类, 那么这里的左端, 从而右端必为 0; 如果 ω 为第二类, 则它们可由那些初始量有理表出; 在一般情形结果是一样的但可能需要添加一些对数项. 从本质上说这是阿贝尔的定理. 如果在右端使用不同于 λ_i 的路径, 它的值仅仅只改动了 ω 的一些周期.

对欧拉的椭圆积分理论的 (以及对于法尼亚诺对同一课题更早的研究的) 相关情形是曲线 Γ 由方程 $y^2 = F(x)$ 定义, 其中 F 为三或四次没有重根的多项式

(参看第二章附录 II); 于是 Γ 的亏格为 1, x 在 Γ 上为二阶; 在差一个常数因子下, 在 Γ 上有一个也只有一个第一类微分, 它由 $\omega = dx/y$ 给出; 它没有零点. 设 $A+N$, $B+M$ 为 Γ 上两个等价的除子; 于是, 由阿贝尔定理, 我们有

$$(1) \qquad \int_A^M \omega = \int_B^N \omega,$$

或者适当地选取积分路径, 等价于

$$(2) \qquad \int_A^N \omega = \int_A^M \omega + \int_A^B \omega;$$

不然的话, 两端会差一个 ω 的周期. 如果 ω 换作了一个第二类或第三类的微分 ω', 那么, 出于同一理由, 两端的差在一个 ω' 的周期下, 可用初始量的有理和对数函数表达; 如果 ω' 是第二类的, 它则可以表示为一个有理函数. 至于条件 $A+N \sim B+M$, 也可写成 $N \sim M+B-A$, 或者用在第二章附录 II 中解释过的记号, 当 A 取为原点时写作 $N = M \dotplus B$. 按照在那里所概述的一般性理论, N 可以用 A, B, M 有理地表达; 不久将要看到, 欧拉得到了对此的显式公式, 而且或许这是他对于椭圆积分课题的主要发现吧.

在经典的椭圆积分理论中按照雅可比、阿贝尔以及他们的后继者们, 人们在 Γ 上取沿从起点 A 到终点 M 的路径的积分

$$u = \int_A^M \omega$$

作为独立变量; 对于给定的一个 M, 这定义了模 ω 的一个周期; 可以证明 ω 的这些周期构成复平面 $\mathbb{C}$ 的一个格 L 并且 M 是被模 L 的 u 值所唯一决定; 因此映射 $u \mapsto M$ 决定了从群 $\mathbb{C}/L$ 到 Γ 上点在 $\dotplus$ 运算下的群的同构. 于是 "椭圆函数" 可看成是在 Γ 上的独立变量 u 的有理函数 (它们的定义表明它是个半纯函数). 用 M 和 M' 表达 $M \dotplus M'$ 的代数公式 (分别地, 用 M 表达 $nM = M \dotplus \cdots \dotplus M$) 于是可以看成是对属于 Γ 的椭圆函数的加法 (分别地, 乘法) 公式. 这个支配了整个十九世纪和部分二十世纪对于这个理论的观点对于欧拉关于此课题的工作是不相干的.

再次取 $N = M \dotplus B$; 令 $M = (x,y)$, $N = (x',y')$; 取 A, B 为常数, 并对 (1) 取微分, 我们得到

$$\frac{dx}{y} = \frac{dx'}{y'};$$

这可以表达为, 对于给出的 A 和 B, 映射 $M \mapsto N = M \dotplus B$ 是一个将微分 ω 变到自己的 Γ 的一个自同构. 这样的自同构无疑构成了一个群 $\mathscr{G}$, 它同构于 Γ 的点在运算 $\dotplus$ 下的群; 这个群是单可迁的, 即有一个且只有一个这样的自同构

将一个已知点 P 映到另一个已知点 Q, 这就是说, 由 $B \sim A + Q - P$ 给出的那个.

更一般地, 设 α 为 Γ 上 P 点的邻域到 Q 点的邻域上的一个解析映射; 假定它将 P 映到 Q, 将 ω 变到 ω. 将它与一个将 Q 映到 P 的自同构 $M \mapsto M \dotplus B$ 相结合, 则得到了一个映射 α' , 将 P 的一个邻域映到 P 的一个邻域, 并使 P 和 ω 不变. 设 t 为 Γ 上的一个以 P 为单零点的函数; 取其为 P 点的局部坐标, 我们从而可写为 $\omega = \sum_{i=1}^{\infty} a_i t^{i-1} dt$, 其中 $a_1 \neq 0$, 这是因为 ω 没有零点. 于是它可写成 $\omega = du$, 其中 $u = \sum_{i=1}^{\infty} a_i t^i / i$; 将映射 α' 用局部坐标 u 表述, 我们看到它必为恒同映射, 这是因为它保持 du 和 $u = 0$ 不变. 这证明了一个像 α 那样的映射必定在处处与映射 $M \mapsto M \dotplus B$ 局部地重合. 运用解析开拓或者代数恒等式的守恒原理, 由此可得出结论说, Γ 的每个将 ω 变成自己的自同构必属于上面定义的 $\mathscr{G}$.

只要 $M = (x, y)$ 就令 $f(M) = x$, 则定义了 Γ 上的一个函数 f; 又, 对于 $M = (x, y)$, 记 $M^- = (x, -y)$, 故而 $f(M) = f(M^-)$, 且 $M \mapsto M^-$ 是 Γ 的一个自同构, 它将 ω 变到 $-\omega$. 如果 P 是 Γ 的一个不同于 A, A^- 的点, 则 Γ 的函数

$$\varphi(M) = \frac{f(M) - f(P)}{f(M) - f(A)}$$

具有零点 P, P^- 以及极点 A, A^-, 故对所有的 P 我们有 $P + P^- \sim A + A^-$. 现在再一次取 $N = M \dotplus B$, 即 $N \sim M + B - A$, 并如前面那样, 令 $M = (x, y)$, $N = (x', y')$. 由于 N 有理地依赖于 M, B 及 A, 我们可以表达 $x' = f(N)$ 为 $R(x) + yS(x)$, 其中 R, S 为 x 的有理函数, 其系数有理地依赖于 A 和 B. 设 $\Phi(x, x') = 0$ 为在 $x = f(M)$ 与 $x' = f(N)$ 的不可约关系; 它对于 x' 的次数必为 2 或 1. 另外, 我们有

$$N^- \sim A + A^- - N \sim A + A^- - (M + B - A) \sim B^- + A - M;$$

因此映射 $M \mapsto N^-$ 是个 Γ 的自同构, 将 M 与 N^- 相互交换从而交换了 $x = f(M)$ 和 $x' = f(N^-)$; 因此对于给定的 A 和 B, 关系式 $\Phi(x, x') = 0$ 必定对 x 和 x' 对称, 故可写为欧拉的 "典则形式" (*Eu.*I-20,71 于 E251 中;1753; 参看前面的 §15):

$$\Phi(x, x') = \alpha + 2\beta(x + x') + \gamma(x^2 + x'^2) + 2\delta x x' + 2\varepsilon x x'(x + x') + \zeta x^2 x'^2 = 0,$$

其中的系数有理地依赖于 A 和 B. 容易看出它不可能对 x' 为一次, 因而也不会对 x 为一次, 但须除去一些 B 的特殊值 (更精确地, 对于 $2B \sim 2A$).

如果把它写成为

$$P_0(x)x'^2 + 2P_1(x)x' + P_2(x) = 0,$$

其中 P_0, P_1, P_3 为二次多项式, 于是, 由于它有一个形如 $R(x)+yS(x)$ 的根 x', 则多项式 $P_1^2-P_0P_2$ 必具形式 ρ^2F, 其中 ρ 有理地依赖于 A 和 B 但不依赖于 M. 反之, 假定已然如此, 于是我们有

$$\frac{1}{2}\frac{\partial\Phi}{\partial x'}=P_0(x)x'+P_1(x)=\pm\sqrt{P_1(x)^2-P_0P_2(x)}=\pm\rho\sqrt{F(x)}.$$

因为 Φ 对称, 故我们也有

$$\frac{1}{2}\frac{\partial\Phi}{\partial x}=\pm\rho\sqrt{F(x')}.$$

因此对关系式 $\Phi(x,x')=0$ 微分, 我们得到

$$\pm\frac{dx}{\sqrt{F(x)}}=\pm\frac{dx'}{\sqrt{F(x')}},$$

如果适当选取符号, 它也可以写成

$$\frac{dx}{y}=\frac{dx'}{y'}.$$

用欧拉的话来表达就是: 关系式 $\Phi=0$ 是上述微分方程的一个积分; 由于它包含了一个任意常数 (就是 $f(B)$; 而 A 一旦取了就不再改变), 故它是个 "完全" 解 (即通解).

一个值得注意的特殊情形是 F 具有下面的形式:

$$F(x)=1+mx^2+nx^4;$$

欧拉和勒让德都指出过, 一般的情形经过适当的变换 $x\mapsto(\lambda x+\mu)/(\nu x+\rho)$ 总可以化成这个情形 (参看前面的 §15). 对于每个 $M=(x,y)$, 令 $M^*=(-x,-y)$; 由于 $M\mapsto M^*$ 是 Γ 的自同构, 且将 ω 变到自己, 因此必具有形式 $M\mapsto M\dotplus B_0$, 其中 B_0 为 Γ 的某个点; 因为它的阶为 2, 我们必有 $B_0\dotplus B_0=0$, 即 $2B_0\sim 2A$. 像前面那样, 取 $N=M\dotplus B$, $x=f(M)$, $x'=f(N)$, 故而我们有 $\Phi(x,x')=0$. 自同构 $M\mapsto M^*$ 将 N 映到了 $N^*=M^*\dotplus B$; 我们已经知道 $f(M^*)=-x$, $f(N^*)=-x'$, 故必有 $\Phi(-x,-x')=0$. 因此 Φ 一定具有以下形式:

$$\Phi(x,x')=\alpha+\gamma(x^2+x'^2)+2\delta xx'+\zeta x^2x'^2,$$

这正是欧拉所设定的那样 (参看前面的 §15).

由于点 A 能任意选取, 我们可假定已取 $A=(0,1)$. 令 $B=(a,b)$; 于是关系式 $\Phi=0$ 必定为 $x=f(A)=0$, $x'=f(B)=a$ 所满足; 这给出了 $\alpha=-\gamma a^2$. 另外, 如果 P_0, P_1, P_2 再次设为 Φ 中 x'^2, $2x'$, 1 的系数, 我们则一定有 $P_1^2-P_0P_2=\rho^2F$; 这给出了

$$\alpha\gamma=-\rho^2,\quad \zeta\gamma=-n\rho^2,\quad \delta^2=\gamma^2+\alpha\zeta+m\rho^2$$

(参看 *Eu.*I-20,158–161 于 E261 中;1755). 因为 $\alpha, \gamma, \delta, \zeta, \rho$ 定义到只差一个公因子, 我们可设 $\gamma = -1$. 这给出了如欧拉所发现的

$$\alpha = a^2 = \rho^2, \quad \zeta = na^2, \quad \delta^2 = 1 + ma^2 + na^4 = b^2,$$

$$\Phi(x, x') = a^2 - x^2 - x'^2 + 2\delta xx' + na^2x^2x'^2.$$

(参看前面的 §15). 对 x' 解 $\Phi(x, x') = 0$, 得到

$$x' = \frac{\delta x \pm ay}{1 - na^2x^2}, \quad \delta = \pm b$$

以及用 x', y' 表示 x 的一个相似公式, 这是因为 Φ 是对称的. 这个双重符号可以按下列方式决定, 即观测 N 对称地依赖于 M 和 B, 并且当取 $M = A$ 时它就是 B. 这给出了 $\delta = b$ 从而

$$(3) \qquad x' = \frac{bx + ay}{1 - na^2x^2}.$$

还有一个用 x', y' 表达 x 的类似公式, 并且再一次看出对 $M = A$, $N = B$ 它一定成立, 我们有

$$(4) \qquad x = \frac{bx' - ay'}{1 - na^2x'^2},$$

它当然也可用来以 x, y, a, b 表达 y'. 这些便是欧拉得到的加法和减法公式 (*Eu.*I-20,69 于 E251 中;1753, 等; 参看前面的 §15). 由此, 人们可以以通常的方式推导出乘法公式. 譬如, 对于 $M_2 = M \dotplus M$, 即 $M_2 \sim 2M - A$, 我们只要在加法公式中令 $B = M$, 从而得到

$$x_2 = f(M_2) = \frac{2xy}{1 - nx^4}.$$

相似地, 对于 $\nu > 2$ 定义 M_ν 为 $M_\nu = M \dotplus M_{\nu-1}$, 或者, 等价地, 对于所有 $\nu \geq 2$,

$$M_\nu \sim \nu M - (\nu - 1)A,$$

并反复地应用加法公式, 得到对于所有 ν, 由 x, y 表出的 M_ν 的坐标. 于是由阿贝尔定理

$$\int_A^{M_\nu} \omega = \nu \int_A^M \omega,$$

这里需要适当地选取积分路径, 不然的话, 两端要差一个 ω 的周期.

所有这些都可通过考虑 "双纽线情形" $y^2 = 1 - x^4$ 进行例解, 而它在法尼亚诺的工作和欧拉关于这个课题的早期工作中起过决定性的作用 (参看前面的

§15). 跟随这些作者们, 我们也取实域为基域; 所有平方根都取正的. 双纽线是曲线

$$(x^2+y^2)^2 = x^2 - y^2;$$

为方便起见, 我们只考虑该曲线位于第一象限 $x \geq 0$, $y \geq 0$ 的部分; 它是起点 $O=(0,0)$ 及终点 $P=(1,0)$ 的弧. 这段弧可参数地表示为

$$x = \sqrt{\frac{1}{2}(z^2+z^4)}, \quad y = \sqrt{\frac{1}{2}(z^2-z^4)}, \quad 0 \leq z \leq 1;$$

它的弧长元由

$$ds = \sqrt{dx^2+dy^2} = \frac{|dz|}{\sqrt{1-z^4}}$$

给出 (参看 *Eu.*I-20,91 于 E252 中;1752). 令 $t=\sqrt{1-z^4}$; $(x,y) \mapsto (z,t)$ 是一个 1–1 对应, 它将所考虑的双纽线的这段弧对应到由 $t^2 = 1-z^4$ 给出的曲线 Γ 的 $0 \leq z \leq 1$, $t \geq 0$ 这一段弧上. 在 Γ 上的所有积分都沿这条弧段进行.

Γ 上的加法和减法公式现在由

$$z' = \frac{\pm z\sqrt{1-\zeta^4} + \zeta\sqrt{1-z^4}}{1+\zeta^2 z^2}$$

给出 (*Eu.*I-20,65 于 E251 中;1753). 因此对于给定的 ζ, 映射 $z \mapsto z'$ 将弧长元 ds 变到自己. 对于 $\zeta = 1$, 减法公式给出了映射

$$z \mapsto z_1' = \sqrt{\frac{1-z^2}{1+z^2}},$$

它将 O 和 P 相互映成对方, 而弧 OP 映到自己并保持弧长元. 对于 $\zeta = z$, 我们得到二倍映射

$$z \mapsto z_2 = \frac{2z\sqrt{1-z^2}}{1+z^4},$$

它将 ds 变成了 $2ds$. 这两个映射是法尼亚诺发现的 (*Fag.*II,294,308; 参看 *Eu.*I-20,92–95 于 E252 中;1752); 加法公式则首先由欧拉得到 (*Eu.*I-20,53–64 于 E251 中;1753; 参看 *Eu.*I-20,100 于 E252 中;1752). 法尼亚诺发现, 如果 M 是双纽线的弧 OP 上任一点, 映射 $z \mapsto z_1'$ 将弧 OM 映到一条有相同长度的弧 PM' 上; 使 OQ 与 QP 长度相等的点 Q 可以由令 $z = z_1'$ 或者 $z_2 = 1$ 得到, 从而由 $z^2 = \sqrt{2}-1$ 给出; 如果 M 在弧 OQ 上, 映射 $z \mapsto z_2$ 将 OM 映到具二倍长的一段弧上.

有点意思的是, 法尼亚诺得到二倍公式 $z \mapsto z_2$ 当然没有用加法公式, 他还不拥有它, 而是 (*Fag.*II,305–307) 结合了两个映射:

$$z \mapsto u = \frac{z\sqrt{2}}{\sqrt{1-z^4}}, \quad u \mapsto z_2 = \frac{u\sqrt{2}}{1+u^4},$$

对此我们有

$$\frac{du}{\sqrt{1+u^4}}=\frac{dz\sqrt{2}}{\sqrt{1-z^4}},\quad \frac{dz_2}{\sqrt{1-z_2^4}}=\frac{du\sqrt{2}}{\sqrt{1+u^4}}.$$

这些公式定义了“兰登变换”, 即在曲线 $t^2=1-z^4$ 与 $w^2=1+u^4$ 之间的一个二次变换 (或用现代语言, 一个同源); 用 ηu 置换 u, 其中 η 是八次单位根 $\eta=(1+i)/\sqrt{2}$, 可以得到在曲线 $t^2=1-z^4$ 上乘以 $1\pm i$ 的复乘积公式. 这是法尼亚诺的工作的一个方面, 它未曾引起欧拉的注意, 但在阿贝尔那里它却获得了十分可观的重要性.

最后, 考虑由方程 $y^2=ax^2+b$ 给出的圆锥截线 C, 其中 $b\neq 0,\ a\neq 0,-1$; 对于 $a<0$ 它是椭圆, 对 $a>0$ 是它双曲线.

它的弧长元由

$$ds=\sqrt{\frac{1+qx^2}{1+px^2}}|dx|$$

给出, 其中 $p=a/b,\ q=(a+a^2)/b$. 如果我们记由

$$z^2=(1+px^2)(1+qx^2)$$

定义的曲线为 Γ, 那么 ds 是 Γ 上的一个第二类微分, 并且我们有了在曲线 C 的点 $\{(x,y)\mid x\geq 0,y\geq 0\}$ 与 Γ 中的点 $\{x\geq 0,\ ax^2+b\geq 0,\ z\geq 0\}$ 之间的一个 1–1 对应. 人们现在可以完全像双纽线情形那样进行, 但由于现在的弧长元是第二类微分, 根据阿贝尔定理, 需要有些变化, 这应除外.

举情形 $b>0,\ 0>a>-1$ 为例; 它对应一个椭圆; 在这里我们来处理椭圆的弧 $x\geq 0,\ y\geq 0$, 起点 $P=(0,\sqrt{b})$, 终点 $Q=(\alpha,0)$, 其中我们已令 $\alpha=\sqrt{-(b/a)}$; P 和 Q 分别对应了 Γ 上的点 $(0,1)$ 与 $(\alpha,0)$. 将减法公式 (4) 应用到 Γ 的点 (x,z) 和 $(\alpha,0)$ 上 (分别以 $x,x',\alpha,0,pq$ 代替 x',x,a,b,n); 我们得到

$$x'=\alpha\sqrt{\frac{1+px^2}{1+qx^2}},$$

它决定了一个从椭圆的弧 PQ 到自己的映射 $x\mapsto x'$, 或者更准确地说, 是到 QP 上的映射, 因为它将 P 和 Q 相互交换; x 与 x' 间的关系也可写成

$$1+p(x^2+x'^2)+pqx^2x'^2=0,$$

这当然是记为 $\Phi=0$ 的那个关系的特殊情形. 将其微分得到

$$(1+qx'^2)xdx+(1+qx^2)x'dx'=0,$$

它表明 $x \mapsto x'$ 像所期待的那样, 是从 PQ 到 QP 的一个 1–1 映射. 这可写为

$$\frac{dx}{x'} + \frac{dx'}{x} + qd(xx') = 0.$$

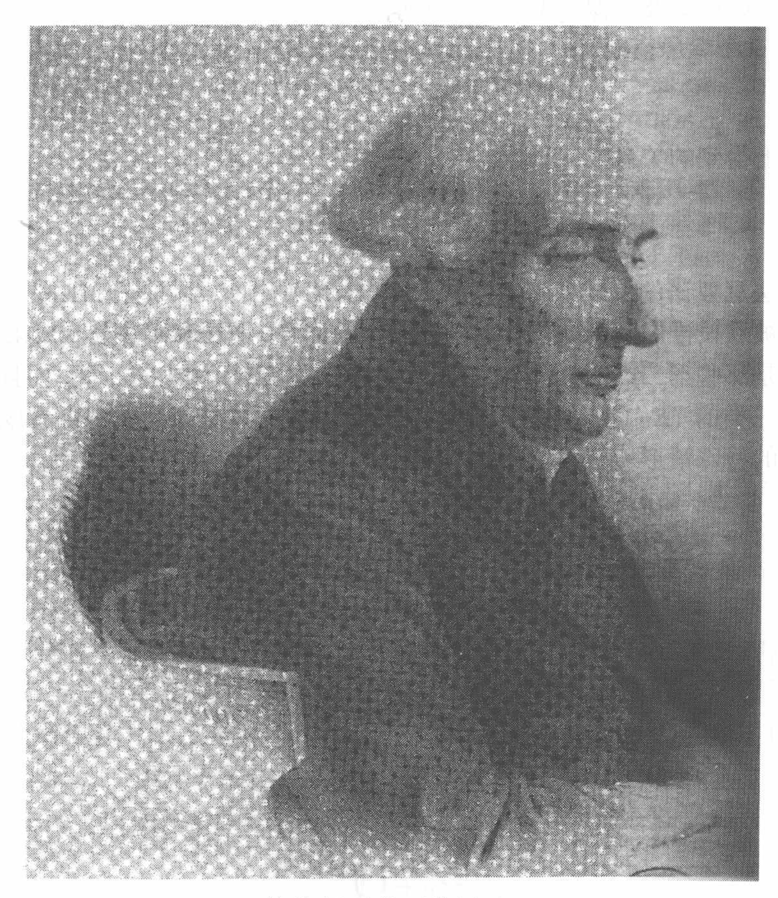
与此同时 PQ 上的弧长元可写为 $ds = \alpha(|dx|/x')$, 从而它在映射 $x \mapsto x'$ 下变成了 $ds' = \alpha(|dx'|/x)$. 设 $M = (x, y)$ 为 PQ 的任一点, 设 M' 为其在 $x \mapsto x'$ 下的像; 于是弧 PM 及其像 QM' 的长分别有

$$\lambda = \alpha \int_0^x \frac{dx}{x'}, \quad \lambda' = -\alpha \int_0^x \frac{dx'}{x};$$

根据以上得到的关系式, 这给出了

$$\lambda' - \lambda = q\alpha xx'.$$

这也是法尼亚诺的发现 (*Fag.*II,287–289; 参看 *Eu.*I-20,82–90 于 E252 中;1752). 它最终被欧拉推广到所有包含有椭圆积分的加法、减法和乘法公式成果的地方, 不仅仅是那些第二类的微分 (*Eu.*I-20,156–158 于 E261 中;1775, 等), 而且甚至是那些第三类的 (*Eu.*I-21,39–56=E581;1775). 所有这些结果当然都可看成是阿贝尔定理的特殊情形.



拉格朗日像 (雕版画)

第四章　过渡时期: 拉格朗日与勒让德

---

§4.1　拉格朗日的生平

在 1745 年, 欧拉被他的年迈的老师约翰 · 伯努利赞誉为 "*mathematicorum princeps* (数学王子)", 数学家的首席 (参看第三章 §3). 到了 1775 年, 欧拉清楚感到要准备将这个称号传给拉格朗日了. 他写信给他这位年轻的同事说 "由本世纪最杰出的数学家作为我的柏林继任者, 这是对我最大的奉承" (索引同上, 第三章 §9). 这也确是那时科学界的广泛预言. 1793 年, 拉瓦锡*1 (Lavoisier) 代表他的朋友们 (*Lag.*XIV,314–315) 向国民大会递交了一份正式申请, 以认定 "*Le célèbre Lagrange, le premier des géomètres* (著名的拉格朗日, 首席数学家)" 指的是拉格朗日; 这发生在雅各比恐怖时期, 而拉瓦锡自己后来也成了这个时期的牺牲品. 到了下一个世纪, "*princeps mathematicorum*" 这个称号由高斯的同胞们一致赞同地赋予了高斯. 从那以后这个称号一直再没有被用过.

拉格朗日于 1736 年生于都灵, 在他出生登记的名字是 Giuseppe Lodivico Lagrangia. 至少就他的父系一方来说, 他具有法国血统, 而拉格朗日从来就没有使用过他的意大利名字; 在他的信件中他的签名总是 Louis (或者 Lodovico, 或者 Luigi) de la Grange (或者 La Grange), 而后又有 Joseph Louis Lagrange 或者干脆签成 Lagrange. 在萨伏依 (Savoy) 王室统治下的皮耶特蒙 (Piedmont), 大部分都是双语地区, 从而拉格朗日同等地掌握了法语和意大利语: 他曾告诉过达

---

*1 1743–1794, 法国化学家, 现代化学的奠基人. 在法国大革命时期任有要职, 后在雅各比 "红色恐怖" 下, 因人诬告被斩首.

朗贝尔 (*Lag.*XIII,88;1767) 他最喜欢的诗人是阿里奥斯托*2 (Ariosto).

他接受的是一种基于经典的传统的教育; 就数学而言他必定几乎全靠了自己. 意大利的光辉数学传统在那时也仅仅是一个回忆了. 甚至法尼亚诺, 这位在地方小镇 Senigallia 度日的人, 也只能给予拉格朗日一些形式的鼓励的话, 那时拉格朗日十八岁, 他想与法尼亚诺开始通信以从中希望得到更多的知识 (*Fag.*III, 179–209;1754). 就在 1754 这同一年, 他自己决定写信给伟大的欧拉, 但没有回信.

下一年所有的事开始改变了. 1755 年 9 月 (参看 *Eu.*IV A-5,378=*Lag.* XIV, 147), 他被任命到都灵炮校的数学和力学的教学职位上, 在那里他似乎有一些有才能的学生, 而且大部分都比他的年纪大. 与此同时他对于欧拉著作的学习也结出了成果. 1755 年 8 月 12 日他给欧拉写了如下的信:

"*Meditanti mihi assidue...praeclarissimum librum tuum de methodo maximorum et mimimorum ad lineas curvas applicata, factum tandem est, ut...inciderim in viam longe breviorem problemata huiuscemodi resolvendi...Quanquam enim merito haesitandum fuerat, an mihi, qui obscuri adhuc nominis sum, te tantum virum, omni pene scientiarum genere clarissimum, interpellare liceret; maximus tamen, ac plane singularis affectus meus in te ex operum tuorum studio iam pridem conceptus, effecit, ut opportunam hanc illius tibi quomodocumque testandi occasionem...de manibus dimittere nullo modo potuerim*" ["经过对您的最光辉的关于极大极小方法用于曲线情形的书的刻苦思索, 我终于被引导到了解决那类问题的一条捷径上……我十分犹豫, 是否像我这样一个不为人知的人仍然应该去接近一个您那样崇高的, 在几乎所有科学分支中有如此高声誉的人; 然而长时间以来通过学习您的著作让我对您怀有极大和独特的情感, 这使我不可能不抓住这个多少能吐露这些情感的机会": *Eu.*IV A-5,366=*Lag.*XIV,138–139]. 伴随该信的还有关于是那个实际上创建了经典变分学的简短概述.

欧拉的回应必定远远超出了拉格朗日的预想. 不仅仅它迅速和大度, 它还充满了热情. 欧拉写给他的年轻的通信人说: "你似乎已将极大极小理论带到了差不多是最高的完善程度; 我羡慕你深邃无边的洞察力" ["*...theoriam maximorum ac minimorum ad summun fere perfectionis fastigium erexisse videris; eximiam ingenii tui sagacitatem satis admirari non possum*": *Eu.*IV A-5,375=*Lag.* XIV,144;1755 年 9 月 6 日]. 下一年, 在他的坚持推荐下, 拉格朗日成了柏林科学院的一名通讯院士, 并已形成了要为他找一个合适职位的计划. 七年战争和毛佩尔退斯*3 (Maupertuis) 的逝世使这些打算化为乌有.

---

*2 1474—1533, 意大利诗人, 以长篇叙事诗《疯狂的奥兰多》而知名.
*3 1698—1759, 德国数学家、哲学家、作家, 当时的柏林科学院院长.

随后的十年, 对拉格朗日来说, 是 "刻苦思索" 的十年, 唯一打断他的是一次到巴黎的访问. 他受到了尊贵的那不勒斯外交官、Caraccioli 侯爵的邀请, 并由其陪同到了巴黎和伦敦, 他在 1763 年 11 月离开都灵, 但在巴黎得了重病, 不能继续前往英国. 1764 年 5 月他返回都灵, 途中在日内瓦停留并会见了在 Ferney 的伏尔泰. 在巴黎他会见了克莱罗, 拉朗德*4 (Lalande), 达朗贝尔, 孔多塞*5(Condorcet) 所有这些法国数学家 (参看 *Lag.*XIV,14). 克莱罗向丹尼尔 · 伯努利是这样描述他的: "*un jeune homme très singulier tant par ses talens que par sa modestie; son caractère est doux et mélancolique; il ne connoît d'autre plaisir que l'étude*" ["一位年轻人, 他的才能比起他的谦逊来更为突出; 他的气质是温和和忧郁的; 除了学习研究, 他不知还有其他什么令他快乐的事": *Eu.*IV A-5,330, 注 [2]; 1763 年 12 月 2 日]. 他已经开始与达朗贝尔通信 (*Lag.*XIII,3–4;1759), 起初更多是些形式上的话; 他们在巴黎相识, 并很快就发展到了亲密友谊的阶段, 这个友谊延续到 1783 年达朗贝尔逝世, 一直未曾中断.

在 1766 年欧拉离开柏林去到彼得堡的时候, 事情变得明显不过: 除了拉格朗日没有别的任何人有资格填充他的位置; 欧拉和达朗贝尔持有同样的观点, 腓特烈大帝也很快被说服了. 拉格朗日欣然接受了这一切, 这是因为在都灵, 除了从 1755 年以来就有的要改善他十分卑微的职位的空洞许诺外什么也没有 (参看 *Lag.* XIII,65;1766). 他与 1766 年出发到柏林; 途中拜访了在巴黎的朋友达朗贝尔, 和伦敦的 Caraccioli 侯爵; 10 月在汉堡登岸. 第二年, 由于不喜欢在一个陌生环境中过孤独的单身汉生活, 他写信给他在都灵的一个女性亲戚并在 1767 年 9 月与她结婚; 他向达朗贝尔把此事说成是纯粹为了图方便, 并赞扬了他的妻子是 "一个出色的家庭主妇, 没有任何一点权利的要求" (*Lag.*XIII, 143;1769). 随后的生活, 除了偶尔出现的健康问题外, 似乎是平静的, 不受打扰的, 直到他在柏林逗留的后期他的妻子患了重病为止. 她死于 1783 年, 而达朗贝尔在他临终的病榻上仍能口述一段对他朋友表达同情的感人的最后话语 (*Lag.*XIII,377). 欧拉的死也发生在这同一年.

有一段时间拉格朗日几乎没有学术上的伙伴关系; 兰伯特*6 (Lambert) 是欧拉在离开柏林科学院前不久为该院录用的, 尽管有着粗俗的举止和外貌, 他成了拉格朗日的好朋友; 他也于 1777 年英年早逝 (参看 *Lag.*XIII,333-334). 1786 年国王的逝世夺走了科学院的奠基人和保护者. 次年的 5 月, 拉格朗日永远地离开了柏林, 让自己定居在巴黎. 在那时当他刚对那里的朋友和同事感到信任时,

*4 1732—1807, 法国数学家、天文学家, 曾主持完成著名的四卷本数学史《*Histoire des mathématiques*》的后两卷.

*5 1743—1794, 法国数学家、哲学家, 以 "孔多塞悖论" 留名.

*6 1728—1777, 德国数学家, 第一个给出 π 是无理数的严格证明.

他竟失去了对数学研究的感觉 (参看由德朗布尔 (Delambre)*7所写的他的 "祭文", *Lag.*I,p.XXXVII). 他此时刚刚才过了五十岁.

他的余生整体上是快乐的. 他的最亲近的同事们成了他的亲密朋友; 1792 年他与他的一个朋友, 天文学家 Le Monnier 的年轻女儿结婚; 她的关爱和虔诚支撑着他直到生命的最后一刻. 他起初以一种带有同情的兴趣, 后来越来越感到惊恐地看待这一场革命, 这段所谓的恐怖时期使他失去了两个最好的朋友 (拉瓦锡和孔多塞). 在这最坏的时期过去以后, 他的价值又得到了认可. 他在巴黎师范学院和巴黎综合理工学院的教学, 使他时不时研究和写出一些可追溯到他 1754 年的《*début*》中的老的想法的东西——这是一本关于函数理论的书 (它构成了他 1797 年的《*Théorie des Fonctions Analytiques*》和他 1806 年的《*Leçon sur le calcul des fonctions*》的主要内容: *Lag.*IX,X), 以及编写了他 1798 年的《*Traité de la résolution des équations numériques*》(*Lag.*VIII). 他也保持着对数学的最新进展的兴趣; 1804 年, 他向高斯表达了对其 1801 年的《*Disquisitiones Arithmeticae*》的钦佩之情:

"*Vos Disquisitiones vous ont mis tout de suite au rang des premiers géomètres ...J'ai depuis longtemps abandonné ces sortes de recherches, mais elles ont conservé beaucoup d'attrait pour moi, et je me contente maintenant de jouir sur cette matière, comme sur plusieurs autres, du fruit des veilles d'autrui...*" ["您的《*Disquisitiones*》立刻将您放到最高层几何学家的同一水平上…… 长期以来我已放弃了这一类的研究, 但它们对我仍保持了很大的吸引力, 对我来说, 关于这些事与关于许多其他事一样, 享受着别人的劳动成果, 这就足够了": *Lag.*XIV,299; 参看 *Lag.*XIV, 300;1808]. 或许他满意地感觉到了年轻的高斯给予他的恭维: 在宣布确立高斯为拉格朗日的合法继任者后, 高斯把他的名著的拉丁文版的标题写成与拉格朗日 1775 年的伟大著作的谦逊的标题一样: *Recherches d'Arithmétiques.*

在充满了拿破仑所给荣誉的晚期生活中, 他从事于修订他 1788 年的《*Méchanique Analytique*》的工作 (*Lag.*XI–XII), 这个他不可能做完的任务似乎耗尽了他的精力. 尽管身患致命的疾病, 1813 年 4 月 8 日, 他进行了一次与他的朋友们的长谈, 包括蒙日*8 (Monge), 拉塞佩德*9 (Lacépède) 和 Chaptal, 按照德兰伯所讲 (*Lag.*I,XLV), 这是一次真正的苏格拉底式的对话, 在那里他回顾了过去并迎接他即将来到的终点. 在此后不久他便失去了意识, 两天后便辞世而去了.

---

*7 1749—1822, 法国数学家、天文学家, 时任巴黎天文台台长.

*8 1746—1818, 法国著名的数学家, 曾任海军部长, 是法国大革命时期学术界的领导人物, 画法几何创始人之一.

*9 1756—1825, 法国博物学家.

§4.2 拉格朗日与数论

由于其过度的谦虚和自卑, 拉格朗日在多个方面与欧拉完全不同, 欧拉对于自己的, 同样也对同代人的发现充满火一般的热情, 从无限制. 拉格朗日在一次写给拉普拉斯的信中, 显然是真诚地说道, 他 "在其他人的工作中比在自己中的得到更多的愉悦, 而对后者总不满意"["*je jouis beaucoup plus des travaux des autres que des miens, dont je suis toujours mécontent*": *Lag.*XIV,71;1777]. 相似地, 对于他的一篇关于天体力学的文章他写信给孔多塞说: "请完全确信我对于我的微薄成果没有附加任何要求, 还没有一个人比我在任何事情上要求的更少" ["*je vous prie d'être intimement convaincu que je n'attache aucun prix à mes faibles productions, et qu'on ne saurait avoir moins de prétentions que je n'en ai en quoi que ce soit*":*Lag.* XIV,15;1773].

拉格朗日最好的工作中, 许多或者较大部分都是直接由欧拉的工作激发的, 他的确对这些工作许多年来一直在进行 "刻苦思索" (索引同上, §I), 对此, 1764 年拉朗德曾写信给欧拉说, 拉格朗日作为一个年轻人已经 "记熟了它们, 直到最微小的细节"(*Eu.* IV A-5,330, 注 [2]). 这特别可用到拉格朗日的数论工作上 (参看前面的第三章§6), 而这只是一个在 1768 年才吸引他的主动兴趣的课题 (参看他给达朗贝尔的信,*Lag.*XIII,118–119;1768) 而从事它则不超过十年. 他在算术方面的著述有如下几部分:

(A) 一篇早期关于佩尔方程的文章 (*Lag.*I,671–731, 于 1768 年夏季写成并送到都灵; 它包含了被第一次写出并交付出版的关于佩尔方程总有一个解从而就有无穷多个解的事实 (这可能已被费马所证明; 参看第二章 §13). 后来拉格朗日批评它是 "非常长且极其不直接" (*Lag.*VII,159=*Eu.*I-1,632, 第 84 篇); 使他恼火的是它一直到 1773 年才发表; 那时它已被他的后来的工作所取代.

(B) 在 1768,1769 以及 1770 年提交给柏林科学院的三篇文章 (*Lag.*VII,377-535,581–652,655–726), 主要处理了连分式和它们对解丢番图方程的应用. 这包含了对于佩尔方程的一个确定性的处理 (*Lag.*II,494–496), 从实质上说, 它等价于我们在第二章 §13 中所叙述的那个; 对如下事实的一个证明, 即所有的二次无理数均具有周期连分式 (*Lag.*II,603–615; 参看前面的第三章§12); 求方程 $z^2 = Ax^2 + By^2$ 解的一个高度原创性的方法 (*Lag.*II,383–399), 它已在第二章§14 中有所综述; 以及求所有二元二次方程整数解的一个方法 (*Lag.*II,655–726). 也包括了一个声称能给出对所有方程 $F(x, y) = a$ 的一个整数解的方法, 其中的 F 为任意 n 次齐次多项式 (*Lag.*II,662–696); 正如勒让德在他 1798 年的《*Essai sur la Théorie des Nombres*》(第一部,§XV,Rem.III,no.126) 中指出的, 这个方法对 $n > 2$ 无效.

(C) 在 (B) 中所列的三篇文章是在拉格朗日收到欧拉的《代数学》之前 (参看第三章§5(c)) 写成的. 该书一到手, 他就有了让他在柏林的年轻同事约翰 · 伯努利三世 (欧拉老师约翰一世的孙子) 将它翻译成法文的打算, 与此译本相随的是前面提到的那三篇文章主要内容的一个改进版本. 这被迅速地完成了, 次年手稿便被送交给里昂的出版商 (参看 *Lag.*XIV,4;1771); 在 1773 年 6 月以两卷本形式问世. 拉格朗日的贡献构成第二卷的 369 页到 658 页 (=*Lag.*XII,5–180=*Eu.* I-1,499–651), 其标题是 "附件 (*Additions*), 关于不定分析 (*De l'Analyse indéterminée*)"

(D) 拉格朗日对于费马关于四平方和定理的证明 (*Lag.*III,189–201; 参看第三章§11); 发表在柏林的 1772 年的《*Memoirs*》中.

(E) 威尔逊定理的一个证明 (*Lag.*III,425–438; 参看第二章§7); 这是在 1771 年 5 月向科学院宣读的, 发表在柏林 1771 年的《*Memoirs*》中, 并在欧拉给拉格朗日的信中有所评论 (*Eu.*IV A-5,496=*Lag.*XIV,235–240;1773; 参看第三章§6).

(F) 拉格朗日关于二元二次型的伟大著作《*Recherches d'Arithémetique*》, 出版于 1775 年的柏林《*Memoires*》中 (*Lag.*III,697–758; 参看第三章§9), 其第二部分——更准确说是一个补充——也于 1777 年在那里出版 (*Lag.*III,759–795).

(G) 最后是一个对丢番图方程 $y^2 = x^3 - 2x$, 或者等价地 $X^4 - 2Y^4 = \pm Z^2$ 的处理, 这个问题源自费马的工作 (参看第二章§15 以及附录 V), 后来又被欧拉考虑过 (参看第三章§16). 这完全是费马的无穷下降法的一个做得仔细的好习题, 但却是第一次应用到亏格 1 且秩 > 0 (即具有无穷多个解) 的方程. 这也是于 1777 年向科学院宣读的, 并同年在那里发表 (*Lag.*IV,377–398).

§4.3 不定方程

上面列出来的是拉格朗日在算术方面的绝大部分贡献, 它们处理的问题已经为费马和欧拉考虑过; 这些东西也已经在第一章和第二章做了还算详细的讨论, 就没有必要在此重复了. 我们也忍住不去叙述拉格朗日对于连分式之类的贡献, 以及将此理论应用到代数方程的数值解上和到次数 > 2 的不定方程上, 因为这些属于所谓的 "丢番图逼近" 而非真正的数论. 另一方面拉格朗日在二元二次型方面的工作应该有一个比在第三章的 §9 所给出的要更加彻底的描述, 在第三章那里我们只是通过年迈欧拉的失明的双眼来看它的.

1768 年在向达朗贝尔宣布他关于不定方程的第一篇大部头论文时 (列在 §2 的 (B) 中那些的第一篇), 他写道, 他已穷尽了两个未知量的二次方程的分式解或整数解这个课题 ["*Je crois avoir entièrement épuisé cette matière, sur laquelle M.Euler paraît s'être vainement exercé*":*Lag.*XIII,125;1768 年 12 月 6 日, 几星

期后他又写道: “*Je crois n'avoir presque rien laissé à désirer sur ce sujet*”: *Lag.*XIII,128;1769 年 2 月 28 日]. 当然他正确地指出, 欧拉在处理这些问题时总是不得不要使他事先知道一个解 (*Lag.*II,378–379;1768 以及 *Lag.*XIII,128;1769 年; 参看第三章§8), 反之, 他自己的方法则完全是有效的而没有任何限制. 但是他很快发现还没有给这个课题下个定论; 在 1770 年他已经发表了他的解决方法的有变化的版本, 标题是 “*Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers* (求不定问题整数解的新方法)”(*Lag.*II,655–726). 下一年, 他仍旧在研究另外的不同方式以便放进他为欧拉《代数学》写的 “附件” 中, 包括, 由于受到下降法的启示 (按他的说法), 他用它来求方程 $z^2 = Ax^2 + By^2$ 的有理解的方法; 在这里他引进了具有如此深远意义的一个新思想, 它从此以后便支配了这个二次型的课题; 用现代的语言表达就是, 它在于一个等价概念, 给定了判别式的二次型按照它分成了类, 而这些类又与简约过程相关联, 该过程则表明了类数是有限的 (*Lag.*II,125–126=*Eu*,I-1,603,Art.70).

在 “附件” 中这个思想仅只提了出来, 并没有强调它. 几年之后, 在更多意识到它的涵盖之广后, 拉格朗日将他 1775 年的整部《*Recherches*》都专门用于它. 我们已经看到欧拉对于他的热情祝贺并不失时机地按自己的方式写了对它的概要 (第三章§9).

§4.4 拉格朗日的二元二次型理论

可以理解, 在《*Recherches*》中给欧拉印象最深刻的要数它包含了对某些事实的证明, 而这些事实是他年轻时依靠经验发现的 (参看第三章§9); 对此他的托词是说, 这是拉格朗日自己在讨论他的主要思想的结果时首要强调的方面. 为了对拉格朗日做到完全公正, 人们就必须根据由它所激发的后续的发展, 特别是高斯及其后继者的工作去观察他的论文集.

费马, 这位二元二次型的创建人从没有走出过 $X^2 \pm AY^2$ 这种类型的几个特殊情形的范围. 欧拉则系统地考虑了 $mX^2 + nY^2$ 这种类型的形式, 除了在处理 $X^2 + 3Y^2$ 时不得不考虑形式 $X^2 + XY + Y^2$ 外, 再无其他 (参看第三章§8). 拉格朗日的起步, 实际是重大的一步, 便意识到一个协调一致的一般性理论需要对所有的形式 $aX^2 + bXY + cY^2$ 同时考虑.

或许在我们看来, 相当显然然而却相当基本的是对如下事实的认识, 即只要有一个关系式

$$(1) \qquad F(X,Y) = f(\alpha X + \beta Y, \gamma X + \delta Y),$$

两个这样的形式 f, F 便 “代表” 了同一个整数 (即方程 $f(x,y) = m$, $F(x,y) =$

m 对同一个 m 值有整数解), 这里的 $\alpha, \beta, \gamma, \delta$ 是满足 $\alpha\delta - \beta\gamma = \pm 1$ 的整数. 用现代术语, 说的就是变换

$$(2) \qquad (X, Y) \mapsto (\alpha X + \beta Y, \gamma X + \delta Y)$$

可逆, 其中的 α, β, γ, δ 如上, (2) 的逆是变换

$$(X, Y) \mapsto (\pm(\delta X - \beta Y), \pm(-\gamma X + \alpha Y)).$$

对于如上那样关联的形式 f, F, 拉格朗日像通常那样不愿意引进新的概念和术语, 他宁愿用不合适的词语 "可以相互转换的形式"; 高斯为它们引进了 "*等价形式*", 它被一直沿用至今. 拉格朗日表明这样的形式具有相同的判别式 $b^2 - 4ac$; 他也充分注意到它们之间的关系的确是在现代意义下的 "一个等价关系", 即它是对称的, 传递的; 用现代语言等于是说变换 (2) 构成了一个群, 就是说, 整数 x, y 构成的向量 (x, y) 的加法群的自同构群 $GL(2, \mathbb{Z})$. 为简便起见, 如果 S 是 (2) 中的变换, 我们就记它的行列式 $\alpha\delta - \beta\gamma$ 为 $\det S$, 以 $F = f \circ S$ 记关系式 (1), 以 $\mathscr{G}$ 记群 $GL(2, \mathbb{Z})$. 区分 "正常" 和 "非正常 (improper)" 等价不是拉格朗日做出的也不是稍后的勒让德做的而是更后面的高斯; 它依赖于满足 $\det S = 1$ 的 $\mathscr{G}$ 中的变换 S 构成 $\mathscr{G}$ 的一个指数为 2 的子群 $SL(2, \mathbb{Z})$ 这一事实, 两个等价的形式 f, F 成为 "正常等价" 的是说, 如果在此子群中有一个 S 使得 $F = f \circ S$, 否则则是 "非正常等价".

一旦这个等价概念被弄清, 具有给定判别式的形式便能够被分配成各个类, 两个形式被放进同一个 "拉格朗日"(分别地, "高斯") 类当且仅当它们等价 (分别地, 正常等价); 在这里第一次使用 "类" 这个字的还是在高斯的意义下的. 一个 "拉格朗日" 类或者是个 "高斯" 类, 或者它由两个这样的类组成. 在这里我们使用的 "类" 这个字专指的是拉格朗日意义下的.

还必须指出在拉格朗日与高斯的用法上的另一个不同之处. 对于高斯 二元二次型 (a, b, c) 定义为形式 $aX^2 + 2bXY + cY^2$, 有一个偶数的中间项系数 $2b$, 高斯总是坚持说按它们的 "行列式" $b^2 - ac$ 来进行分类, 这是最恰当的记号. 另一方面, 拉格朗日作为出发点的则是形式 $aX^2 + bXY + cY^2$, 其中 b 可偶可奇, 而有时也事先给出偶的中间系数. 在这里我们以 (a, b, c) 记 "拉格朗日" 形式 $aX^2 + bY^2 + cZ^2$, 称 $b^2 - 4ac$ 为其判别式 (与 b 同为奇偶). 这样的形式在十九世纪大部分时间里从文献中消失之后 (在高斯的影响下), 又在戴德金 (Dedekind) 用二次域的理想理论重新解释二元二次型后, 再次凸显出来. 当然只要不涉及特征 2 的域 (或者环), "拉格朗日" 与 "高斯" 形式之间的也仅仅是记号上的差异而已, 这是因为形式 $f = aX^2 + bXY + cY^2$ 当 b 为奇数时, 若要在高斯理论的架构上考虑它的话总是将它用 $2f$ 替代. 为简便起见, 我们将排除判别式 $b^2 - 4ac = 0$

或者为一平方数的形式 (a,b,c); 这些是可以写成两个整系数线性形式乘积的.

另一个有些重要的观察, 特别由于欧拉以前考虑过的, 涉及关于一个形式 f "正常表示" 的整数问题, 即那些可以写成 $f(x,y)$ 的整数, 其中 x, y 互素; 这些对于两个等价的形式是相同的, 这是因为在 $GL(2,\mathbb{Z})$ 中的一个变换将每个 x, y 互素的数对 (x,y) 映成相似的一对. 对于 $f=(a,b,c)$, 其中 a 与 c 都被 f 正常表示, 因为我们有 $a=f(1,0)$, $c=f(0,1)$; 因此, 如果 $F=(A,B,C)$ 等价于 f, A, C 都被 f 正常表示. 反之, 设 m 为一个被 f 正常表示的整数, 故我们可写成 $m=f(\alpha,\gamma)$, 其中 α 和 γ 互素; 于是存在整数 β, δ 使得 $\alpha\delta-\beta\gamma=1$, 而 m 是在 (1) 定义的形式 F 的 X^2 的系数. 现在让 d 为形式 f 的 "因子", 按照欧拉的意思, 它是由 f 正常表示的一个整数 m 的任一因子, 但须假定与 f 的判别式 D 互素. 于是有等价于 f 的 F, 它的第一个系数为 m, 故我们可写成 $F=(m,n,p)$; 由于 F 与 f 有相同的判别式我们有

$$D=n^2-4mp=n^2-4d(m/d)p;$$

因此 d 是形式 $(d,n,(m/d)p)$ 的第一系数, 其判别式为 D, 并由它正常表示 (参看第三章§9).

如欧拉正确看到的 (参看第三章§9), 拉格朗日的最具决定性的步骤在于证明了每个形式 (a,b,c) 可以用逐次的变换

$$(X,Y)\mapsto(X-rY,Y)$$

和

$$(X,Y)\mapsto(X,Y-sX)$$

变成一个等价的形式 (A,B,C), 使得 $|B|\le|A|$ 以及 $|B|\le|C|$ (*Lag.*VI,125–126=*Eu.*I-1,603–605,Art.70; *Lag.*III.697–700). 他的证明就是在前面第三章 §9 中叙述的那个.

拉格朗日没有对满足上述条件的形式 (A,B,C) 指定一个称呼, 我们就叫它为 "拉格朗日意义下的简约的", 或干脆叫简约的, 只要在目前的背景下不引起混乱就行 (高斯是在有点不同的意义下引进了这个词). 对于这样一个形式, 我们已经看到 (第三章 §9), A, B 和 C 可由 $D=B^2-4AC$ 给出上界, 故容易列出具有给定判别式的所有这些形式; 拉格朗日的证明表明在每个类中至少有一个简约形式. 在第三章的 §9 已叙述过的这个方法将一个给定的形式变换为一个简约形式, 我们可称之为 "拉格朗日简约".

因此, 欧拉没能跟上拉格朗日. 或许他对于在《*Recherches*》中所解决的最后那个问题给予了较低的评价, 否则就是他在这里被所涉及的复杂计算所阻挡. 然

而在拉格朗日和他后继者的眼里, 得到具给定判别式的形式的类的表示 (在严格意义下) 的集合, 即那些形式的集合使它含有且只含有每个类中一个形式的问题, 这是对拉格朗日简约方法的不可或缺的补充. 拉格朗日发明了一个得到等价于一个已知形式的所有简约形式的步骤而不求助于反复试验的方法 (*“sans aucun tâtonnement”: Lag.*III, 737). 明显地, 连续地对具给定判别式所有简约形式的每一个施行这个步骤, 并相应地消去多余的, 就得到所想要的表示的集合.

最初拉格朗日似乎找到了统一的处理所有类的方法, 对此使用了 $GL\,(2,\mathbb{Z})$ 中变换的一种典则的分解; 然而他不久便发现, 形式在这方面按它们的判别式的符号表现得十分不同. 就他所知, 一个形式 f 具有判别式 $D<0$ 当且仅当对于不全为零的整数 x, y 它取的所有值 $f(x,y)$ 有相同的符号; 自高斯起, 称此为*定形式*, 而具 $D>0$ 的为*不定形式*. 明显地, 在定形式中只要考虑那些只具有正值的就够了, 对于这样形式 (a,b,c), a 和 c 必定 >0. 拉格朗日发现, 如果 $F=(A,B,C)$ 为定形式且简约 (“拉格朗日意义” 下), 则除了在变换 $(X,Y)\mapsto(X,\pm Y)$, $(X,Y)\mapsto(Y,\pm X)$ 下的变化形式 $(A,\pm B,C)$, $(C,\pm B,A)$ 外再没有其他等价于 F 的简约形式了. 他对此的证明被后来勒让德的证明给掩盖了 (在他 1798 年的《*Essai*》, 第一部,§VIII), 它既更简单又更不形式化; 我们将在附录 II 中叙述它.

对于不定形式问题更加困难, 在某种意义上说, 更加有意思; 拉格朗日处理他的方法明确地受到了他自己求佩尔方程解的方法的启示, 它的确可以看成是所给出的简约方程为 X^2-NY^2 的特殊情形. 在他的《*Essai*》(第一部,§XIII) 中, 勒让德以更明晰的连分式理论的利用给出了一个拉格朗日解的改进表示; 这后来被高斯改成了他自己的 “正常等价” 的概念 (*Disq.* Art.184–193; 参看在 *Vorlesungen über Zahlentheorie*,ed. R.Dedekind, Braunschweig,1894,§72–§82 中狄利克雷的定表示). 拉格朗日原来的处理将在附录 III 中叙述.

§4.5 勒让德的生平

勒让德 (Adrien–Marie Le Gendre 或者 Legendre) 在 1752 年出生于巴黎, 1833 年逝世于此. 泊松在他的葬礼上说, “让他生命走到尽头的疾病给了他长期而痛苦的折磨, 我们同事们经常提及的愿望是当谈到他时应该只提到他的工作, 它们的确就是他生命的全部”. 但是, 在他逝世的前一年写信给年轻的雅可比祝贺其结婚时, 勒让德曾沉湎于他对自己生活的回忆之中: “ 在一场摧毁了我拥有的可怜财富的血腥革命后, 我结婚时的年纪要比您晚了许多; 我们曾处在十分窘迫的境地和一个真正艰难的时刻, 但我的妻子强有力地帮助我将我的事业向前推进以便…… 获得…… 一些财富, 在后继的革命所带来的损失之

后它所残留的部分仍能适当地照顾到我老年的需要, 以及当我不再需要时我挚爱的妻子的需要. 但我谈自己已经太多了······" [*"Je me suis marié beaucoup plus tard vous et à la suite d'une révolution sanglante qui avait détruit ma petite fortune; nous avons eu de grands embarras et des moments bien difficiles à passer mais ma femme m'a aidé puissamment à restaurer progressivement mes affaires... de manière à me procurer bientôt une existence honorable et une petite fortune dont les débris, après de nouvelles révolutions qui m'ont causé de grandes pertes, suffiront encore pour pourvoir aux besoins de ma vieillesse et suffiront pour pouvoir à ceux de ma femme bien-aimée quand je n'y serai plus. Mais c'est tròp parler de moi..."*:*Jac.*I,460;1632 年 6 月 30 日]. 确实, 在 1792 年他与一个姑娘结了婚, 她还不到他的一半年纪, 而她比他多活了 23 年.

勒让德早年就引起了巴黎的资深数学家的注意. 出身于富有之家的他却接受了在军事学校的一个教师职位并从 1775 年到 1780 年一直从事于此. 1782 年一篇他送到柏林的关于弹道学的获奖文章使拉格朗日向拉普拉斯询问他的情况 (*Lag.*XIV,116;1782), 拉普拉斯的回答高度赞扬了勒让德 (*Lag.*XIV,121;1783); 同年由于拉普拉斯的晋升, 勒让德继他之后作为 "助理"("*adjoint mécanicien*") 任巴黎科学院的副院士 (associate membership); 他自己也在 1785 年得到晋升. 巴黎科学院于 1793 年被废止, 最终作为法兰西学院的一部分得到恢复; 像他向雅可比写的那样, 在法国革命的动乱时期他经历了维持生计的困难, 他从事了各种各样的职位, 这些大体上都归于他在数值计算方面被承认的技巧有关. 1787 年勒让德已经是测地学学术委员会的委员, 他的业务让他去到伦敦, 在那里他成了皇家协会的成员; 1791 年以及再次从 1794 年往后他成了那个最终建立的度量系统的委员会的成员. 1799 年到 1815 年他是巴黎综合理工学院的巡视员, 这在那时是一个重要的职位, 但说不上显赫. 1813 年继拉普拉斯后在经度局 (*Bureau des Longitudes*) 任职, 直到逝世.

泊松在勒让德葬礼上发表的悼词中有一个意见可能不会赢得他以后的同事们的赞同. 他说:"*Les questions relatives aux propriétés des nombres, isolées de toute application, n'ont qu'un seul attrait, à la vérité bien puissant sur les mathématiciens: l'extréme difficulté qu'elles présentent*" ["必须承认, 对于数学家来说, 那些远离应用的, 归属于数的性质的问题, 具有唯一的, 也是强大的吸引力: 它们极其困难"]. 这可以与勒让德在 1798 年他的《*Essai*》的前言中自己关于数论的话相对照: "*Il est croire ...qu'Euler avoit un goût particulier pour ce genre de recherches, et qu'il s'y livroit avec une sorte de passion, comme il arrive à presque tous ceux qui s'en occupent*"["看起来······ 欧拉对于这样的研究有一种特殊的爱好, 而且以一种充满激情的迷恋来从事它们, 这也像对几乎所有与它

ESSAI

SUR LA THÉORIE

DES NOMBRES;

Par A. M. LE GENDRE, de l'Institut national.

A PARIS,

Chez DUPRAT, Libraire pour les Mathématiques, quai des Augustins.

AN VI.

《论数论 (*Essai sur la Théorie des Nombres*)》的扉页

们相关的人们所出现的一样": *Essai sur la Théorie des Nombres*, Paris, An VI (=1798),p.vi]. 无疑, 勒让德在写这几句话时, 必定流露出他总保持着的, 对于连同椭圆函数一起的他所钟爱的学科的情感.

§4.6 勒让德的算术工作

勒让德的第一次进入数论的经历是一个长篇论文, 他在 1785 年将它递交给巴黎科学院, 以标题 "*Recherches d'Analyse Indéterminée*(不定分析研究)" 发表在 *Mémoires de Mathématique et de Physique...de l'Académie Royale des Sciences*, Année 1785,pp.465–559 上: 它像年轻的高斯在格丁根大学图书馆发现了这份文献时, 写给他老师 Zimmermann 的 1796 年 5 月的信中所说的那样, 是 "一篇杰出的论文" ["*eine vortreffliche Abhandlung*": 参看 L.Schlesinger, *Ueber Gauss' Arbeiten zur Funktionentheorie*, p.21, 于 *Gau.*X-2 中). 在勒让德写这篇文章时, 欧拉已经逝世而拉格朗日也已停止了在此领域的积极活动. 显然勒让德是他们著作的热情的学生, 这些著作至少包括了欧拉的《*Opuscula Analytica*》的第一卷, 它出版于 1783 年; 在它的 84 页 (=*Eu.*I-3,512 于 E552 中; 参看第三章§8 以及附录 I) 包含有一段如此接近二次互反律的陈述, 以致几乎不能与它区分开来.

随着岁月流转, 勒让德启动了一个更具雄心的计划; 它采用具充分容量的长卷形式, 力求给出对于数论的一个包罗广泛的记述, 不仅包括他自己的研究, 还要包括欧拉和拉格朗日的所有重要发现, 同样还对许多证明不甚确定的结果的列出数据 (以大范围列表的形式). 1798 年它在巴黎发行, 书名为《*Essai sur théorie des nombres*》; 作者在前言中写道:" 我并没有打算提供一个完全的论述, 而仅仅旨在粗略地显示出这个理论的当前状态"["*Je le donne non comme un traité complet, mais simplement comme un essai qui fera connoître á-peu-près l'état actuel de la science*": pp.ix–x].

随着高斯 1801 年的《*Disquisitiones*》的问世, 这部著作经历了内容广泛的修订, 但这并没有影响它的主要面貌; 这使它在 1808 年出了第二版. 首次发表在巴黎科学院的 《*Memoirs*》的补充部分随再版也加了上去. 感觉到自己现在在改进该作品上已尽其全力了 ["*L'ouvrage ayant ainsi reçu tous les perfectionnements que l'auteur a pu lui procurer*":p.v], 这次勒让德让他的书名叫做 "*Théorie des Nombres* (数论)". 在那时, 他的年轻的同代人都清楚知道, 高斯的《*Disquisitiones*》已经把它变得过时了.

据说高斯在发表他的著作时的原则是, 在让公众查看他的建筑前就把脚手架都拆掉. 对于勒让德的数论, 可以公平地说, 常常是在其中脚手架要比实体的砖石结构要多; 甚至基础有时也摇摇摆摆使得访客们感到相当不安全, 尽管勒让

德也时时插上警示标记. 在讨论它的内容时还是从 1785 年的《*Recherches*》开始为好, 在那里事情叙述得更清晰些. 这本论文集共分为四部分, 前两部分只值得最简短地提一下. 第一部分是关于模素数的高次同余问题 (pp.465–490), 只写了欧拉结果的许多容易的推论, 欧拉的这些结果我们已在前面叙述过了 (第三章§6). 第二部分 (pp.490–507) 给出了将一个整系数多项式在 $\mathbb{Q}$ 或 $\mathbb{Q}$ 的二次扩域上分解为较低次因式的步骤.

《*Recherches*》的第三部分 (pp.507–513) 首先 (pp.507–509) 致力于方程 $ax^2+by^2+cz^2=0$ 的拉格朗日的解, 这我们在前面也已叙述过 (第二章§14); 对此它补充了 (pp.509—513) 下述重要判别法的证明, 这是勒让德主要成名的结果之一:

定理. 设 a, b, c 为三个整数, 它们不具有相同的符号, 并使得 abc 不含平方因子. 于是方程

$$ax^2+by^2+cz^2=0$$

有一个不全为 0 的整数解 x, y, z 当且仅当 $-bc$, $-ca$, $-ab$ 分别为模 a, 模 b, 模 c 的二次剩余.

虽然勒让德对此的证明是直截了当的, 但多少有些生造的痕迹; 对于它的另一个证明可参看附录 I (对此方程更完全的处理也可参看狄利克雷的《*Vorlesungen über Zahlentheorie*》,ed. R,Dedekind, Braunschweig 1894,§157).

在第四部分 (pp.513–552) 中, 上面的判别式被应用 (pp.513–523) 到一个一个定理的并未完全成功的证明上, 勒让德后来称这个定理为 "素数间的一个互反定律", 他仍旧以 "(二次) 互反律" 而著名. 它在一个奇素数 p 模另一个奇素数 q 的二次剩余特征标和 q 模 p 的二次特征标之间建立了一个关系. 为了表达它, 勒让德在 1785 年引进了记号 $N^{(p-1)/2}$, 其中 p 是个任意素数, N 为与 p 互素的整数, 它并不像字面上所解释的那样而是表明 $N^{(p-1)/2}$ 模 p 的最小剩余, 它根据 N 是否是模 p 的二次剩余为 $+1$ 或者 -1. 在 1789 年他把这个笨重的又不合适的记号换成了著名的 "勒让德符号"

$$\left(\frac{N}{p}\right),$$

以上面同样的意思定义[1].

在附录 I 中我们将对勒让德的思想是部分成功的理由进行解释. 勒让德所做的是按照 p 和 q 模 4 的值以及 (p/q) 的值区分成 8 种情形; 高斯在对所讨论的这个定律的第一个证明中也是按同样的安排进行考虑的 (*Disq.* 第 136 篇).

[1] 为了打字方便, 在这里除了显示公式外总印成 (N/p).

在它们中每一个情形, 勒让德引进了一个适当的方程

$$ax^2 + by^2 + cz^2 = 0,$$

其中 $a \equiv b \equiv c \equiv 1 \pmod 4$; 它不可能有非平凡解, 这是因为同余式

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod 4$$

无这样的解. 因此, 由勒让德的判别法, $-bc$, $-ca$ 及 $-ab$ 不能同时分别为模 $|a|$, 模 $|b|$, 模 $|c|$ 的二次剩余. 勒让德在每一种情形都试图选取 a, b, c 以引向所要的结论.

首先取 $p \equiv 1$, $q \equiv -1 \pmod 4$, $(p/q) = -1$ 以及方程 $x^2 + py^2 - qz^2 = 0$; 由于 $(-1/q) = -1$, 我们有 $(-p/q) = -1$; 因此 (q/p) 不可能为 1; 它必为 -1 , 故这符合互反律的要求. 同样的推理可用到 $q \equiv q' \equiv -1 \pmod 4$, $(q/q') = 1$ 的情形以及方程 $x^2 - qy^2 - q'z^2 = 0$.

现在取 $q \equiv q' \equiv -1 \pmod 4$, $(q/q') = 1$. 勒让德在这种情形引进了方程 $px^2 - qy^2 - q'z^2 = 0$, 其中 p 是个辅助的素数, 满足条件

$$p \equiv 1 \pmod 4, \ \left(\frac{p}{q}\right) = -1, \ \left(\frac{p}{q'}\right) = -1.$$

假定存在这样一个素数, 并应用前面已证明的结果则推出结论: $(q'/q) = 1$ 要使这个成立, 必须在一个形如

$$\{4qq'x + m \mid x = 0, 1, 2, \cdots\}$$

的一个算术级数中有一个素数, 这里的 m 可取为任意 > 0 且 $< 4qq'$ 的整数, 并 $\equiv 1 \pmod 4$ 以及模 q 和模 q' 为非剩余.

勒让德正确地使自己相信每一个 a 与 b 互素的算术级数 $\{ax+b\}$ 含有无穷多个素数. 他在 1785 年写过 (《*Recherches*》,p.552)“或许有必要严格地证明它”. 他在 1798 年又说 (《*Essai*》,p.220),“但我们不必对此有所怀疑”, 这次他用了一个完全不能使人信服的论证试图来支持他这个陈述 (《*Essai*》,pp.12–16), 后来甚至更糟糕地扩大成《*Théorie des Nombres*》的整整一章 (t.II,§XI,pp.86–104). 这便留给了狄利克雷来证明这个算术级数的定理了: 他在 1837 年用一个完全原创的方法给出了对它的证明 (*Dir.*I,315–342), 而这也是他的主要成就之一; 用此同样的方法他也证明了 (*Dir.*I,499–502), 如果 a, b, c 没有公因子, 则二次型 $ax^2+bxy+cy^2$ 表示了无穷多个素数, 这也是勒让德所提出的一个陈述 (《*Théorie des Nombres*》, t.II,vpp.102–103).

在我们刚讨论过的情形中, 被勒让德当作一类公理的这个算术级数的定理, 至少对于他的论证给出了一些使其合理的外表; 但是还有更糟糕的事出来. 就

举两素数 p 和 p', 两个都 $\equiv 1 \pmod 4$ 的情形吧. 勒让德试图利用方程 $px^2 + p'y^2 - qz^2 = 0$ 来处理它, 其中 q 是个辅助的素数, 它满足

$$q \equiv -1 \pmod 4, \left(\frac{q}{p'}\right) = 1, \left(\frac{p}{q}\right) = -1,$$

或者另外地, 利用 $x^2 + py^2 - p'qz^2 = 0$, 其中 q 满足

$$q \equiv -1 \pmod 4, \left(\frac{p}{q}\right) = -1$$

(《*Recherches*》,pp.519–520;《*Essai*》,pp.216–217, 以及 220–221;《*Théorie des Nombre*》,t.I, pp.233–234). 有这样的一个素数吗? 无疑它的存在性可由狄利克雷定理和互反律得到; 但值得怀疑的是 (如高斯所指出) 它能用其他方式证明. 因此勒让德的方法最终必定陷入一段循环推理之中, 此路不通. 然而这并未阻止他的抱怨, 在一封 1827 年给雅可比的信中, 他既痛苦又不公正地抱怨高斯只 "宣称自己" 发现了互反定律 (*Jac.*I,398). 然而他一定意识到高斯对他的证明的批评是对的; 在他 1830 年的《*Théorie des Nombres*》他选择了保险的做法 (t.II,pp.57–64), 放进了高斯的第三个证明 (参看 *Gau.*II,3–8;1808), 并且, 外加了 (t.II,pp.391–393) 雅可比在他们通信的开始告诉他的对此另外的 "分圆" 法的证明 (*Jac.*I,394;1827).

1785 年的《*Recherches*》的第四部分的剩余部分或者至少它的最有价值的一部分 (pp.531–548) 专门是一系列的观测 (他称它们为 "*quelques remarques assez singulières*(一些十分值得注意的现象)" (p.531); 在他 1798 年的《*Essai*》p.ix 中又称这是 "*l'ébauche d'un théorie entièrement nouvelle* (一个全新理论的草图)"), 他们涉及不仅是整数的而且是二元二次型作为三个平方数和的表示. 这些都给出了包含在这本论文集后面的 (pp.553–559) 表格中的数据; 他写道, "*on peut les regarder comme autant de théorèmes, car quoique je n'en donne pas la démonstration complète* [*sec!*], *ils sont fondés au moins sur une induction trè-étendue*" ["人们可以将它们看成是许多的定理, 因为, 虽然我没有给出对它们的完全证明, 但它们至少是建立在广泛的数据基础之上的": p.531]. 甚至欧拉也不会对这样的事如此的不在乎.

这个概述后来又被扩展到了 1798 年的《*Essai*》的整个第三节 (pp.321–400) 并在 1808 年重版中又加以改写; 到那时这个同样的领域已经在高斯的《*Disquisitiones*》中得到远远更为简明、更坚实、更全面的涵盖 (*Disq.*Art.266–293). 然而, 在格丁根图书馆发现了勒让德的《*Recherches*》几个星期后的 1796 年 7 月, 年轻的高斯便开始着手他的三平方和的研究 (参看他的《日记 (*Tagebuch*)》的 no.17–no.18, *Gau.*X-1,496–497) 仅仅是一个巧合吗? 不管怎样说, 高斯

的第一步 (同上 no.17) 是验证勒让德在 1785 年注意到的那些关系, 这是在一个整数 N 为三个平方数和的表示与某些判别式为 $-N$ 且也可分解为三个平方因子之和的二元二次型之间的关系. 由此人们可以推导出在 N 的三平方数之和表示的个数与行列式为 $-N$ 的二次型的适当的类数之间的关系; 1785 年在按经验发现了这些关系后, 勒让德寻求在 1798 年的《*Essai*》(pp. 366–400) 和以后的一些文章中建立它们; 这特别包括费马著名的断言, 即每个整数是三个 "三角数" 之和 (《*Essai*》,p.399; 参看前面的第二章 §14). 如高斯正确地看出那样, 这些打算使得勒让德陷入了真正的错综复杂的关系之中, 对他来说不太容易从中解脱出来, 而仍然会将他的主要结论置于令人怀疑的境地["*compluribus difficultatibus implicatus est, quae effecerunt ut theoremata palmaria demonstratione rigorosa munire non licuerit*": *Disq.* Addit ad Art. 288–293,*Gau.* I,466]. 当然, 高斯在《*Disquisitiones*》中对这些结果以及其他更多的类似的重要结果给出了完全的证明.

在另外一个很重要的事情上, 勒让德也是高斯的先行者, 这有点超出了高斯愿意承认的程度. 我们曾看到 (参看前面的 §4), 勒让德证明了, 如果 d 是一个二次型的任一 "因子", 则它可由具相同判别式的某个二次型正常表示. 特别地, 设 d 是 X^2+NY^2 的一个 "因子", 即使得 $-N$ 是个模 d 的二次剩余 (参看第三章§8); 于是 d 可以被某个形式 $f=aX^2+2bXY+cY^2$ 正常表示, 其中行列式 $b^2-ac=-N$. 设 b' 为另外的这种因子, 相似地有 f' 表示; 假定 d' 与 d 互素; 由于 $-N$ 为模 d 和模 d' 二次剩余, 于是也是模 dd' 的二次剩余; 因此 dd' 可以被某个形式 F 表示, 它同样具有行列式 $-N$. 正是由于勒让德的过人之处, 认识到 F 之依赖于 f 和 f'; 换句话说, 存在一个形式 F 使得每个由 f, f' 分别正常表示的两个整数的乘积也由 F 正常表示.

为了证明此, 勒让德取了两个形式

$$f(X,Y)=aX^2+2bXY+cY^2,$$
$$f'(X',Y')=a'X'^2+2b'X'Y'+c'Y'^2,$$

它们具有相同的行列式 $\delta=b^2-ac=b'^2-a'c'$. 令 $Z=aX+bY$, $Z'=a'X'+b'Y'$, 他得到

$$af(X,Y)=Z^2-\delta Y^2,\quad a'f'(X',Y')=Z'^2-\delta Y'^2.$$

他把 "婆罗摩笈多 (Brahmagupta) 恒等式" (参看前面的第三章§8) 用于它; 这给出了

$$f(X,Y)f'(X',Y')=\frac{1}{aa'}[(ZZ'\pm\delta YY')^2-\delta(ZY'\pm YZ')^2].$$

上式的右端可以写成 $AU^2+2BUV+CV^2$, 其中已令 $A=aa'$, $C=(B^2-\delta)/A$,

进而令

$$V = ZY' \pm YZ', \quad AU + BV = ZZ' \pm \delta YY'.$$

其中 B 仍需适当决定. 经容易的计算得到 $U = XX' + mYX' + m'XY' + nYY'$, 其中的 m, m', n 由

$$m = \frac{b \mp B}{a}. \quad m' = \frac{b' - B'}{a'} \quad n = mm' \mp C$$

给出 (《*Essai*》, 第四部,§III, no.362–no.369).

现在假定 a 和 a' 互素; 如若不然, 勒让德看出, 可将 f' 换成一个等价的形式满足此条件, 当然假定了 a', $2b'$ 以及 c' 没有公因子. 那么取 $B \equiv \pm b \pmod{a}$, $B \equiv b' \pmod{a'}$; 于是我们有

$$B^2 \equiv b^2 \equiv \delta \pmod{a}, \quad B^2 \equiv b'^2 \equiv \delta \pmod{a'},$$

故而上面公式中的所有系数全为整数. 由于这里的双重符号, 从而勒让德得到两个形式

$$F(U, V) = AU^2 + 2BUV + CV^2,$$

行列式为 $B^2 - AC = \delta$ 以及如下性质: 存在一个恒等式

$$f(X, Y)f'(X', Y') = F[B(X, Y; X', Y'), B'(X, Y; X', Y')],$$

其中 B, B' 为对于 X, Y 和对于 X', Y' 的双线性形式. 婆罗摩笈多恒等式在这里是作为特殊情形出现的; 至少欧拉注意到了另一个形式 (参看他的《代数》,*Eu.*I-1,424,Art.178, 以及前面的第三章§14).

任何一个熟悉高斯的二元二次型复合概念的人就会立即在上面的初等构造中认出它来; 对应于在那些公式中上面那个符号的形式 F (它明显对称地依赖于 f 和 f') 是由 f 和 f' 经 "复合" 导出的. 无疑高斯选来描述他的高斯理论并非精心制作的; 的确, 以致对于《*Disquisitiones*》的读者来说它成了一个障碍物, 直到后来狄利克雷又重新回到非常接近勒让德原来的构造从而恢复了它的简明性 (*Dir.*II,107–114;1851). 高斯是受到勒让德《*Essai*》的启示才发展了他自己的理论的吗? 这似乎至少看起来是有道理的, 尽管高斯说, 直到《*Disquisitiones*》的 "绝大部分"("*maxima pars*":*Gau.*I,7) 付印后他才看到勒让德的书; 实际上他在 1798 年秋天着手研究 "复合"(参看 *Gau.* I,476,Zu Art.234), 那时他访问了在 Helmstedt 的 Pfaff (参看他给 Bolyai的 1798 年 11 月 29 日的信); 或许他可能在那里已看到过《*Essai*》[2].

[2]《*Disquisitiones*》的相关的第 V 节直到很后才付印; 它包含了三元二次型的理论, 高斯在 1799 年 2 月才开始着手 (参看《*Tagebuch*》,no.96,*Gau.*X-1,539) 而且在 1800 年 2 月尚未完成 (参看同上, no.103,*Gau.* X-1,545).

勒让德似乎理所当然地认为他从 f 和 f' 导出的两个形式 F (由于双重符号) 的类只依赖于 f 和 f' 的类; 这并非是十分显然的, 理应给出证明. 但是同时在他的处理与高斯的处理之间有一个实质的区别. 勒让德从不区分正常的与非正常的等价; 他的二次型的类是拉格朗日类 (参看前面的 §4). 因此这让高斯有机会发现 "高斯类" 在复合的运算下构成了一个有限交换群, 从而得出了以上结果. 如果 C 是个 "高斯类", 于是相应的 "拉格朗日类" 或者在群运算的意义下如果有 $C = C^{-1}$, 则为 C, 否则则为 C 与 C^{-1} 的并; 如果 C' 是另一个 "高斯类", 则高斯意义下的复合产生了一个类 CC', 而勒让德的运算产生对应于 CC' 和 CC'^{-1} 这两个的拉格朗日类, 从而是个双值函数, 这解释了在他的公式中的双重符号; 在他的表格 (《*Essai*》的 pp.432–434) 中也出现了这种情形, 他在表中列出了他的运算结果, 譬如对于行列式 −89. 在这方面勒让德或许也错过了他的发现的最有价值的一面.

勒让德在其老年时认可了一件最终使他满意的事. 自高斯的工作后, 费马的被称作的 "大定理", 对于指数大于 4 仍然是对所有算术学家的挑战. 在 1798 年后来又在 1808 年的《*Essai*》中勒让德除了重现费马对指数 4 的证明和欧拉对于指数 3 的证明外也不能再有什么作为了 (参看前面的第二章 §10,§12, 以及第三章的 §14). 但在接下来的十年中, 对这个问题的兴趣在巴黎又恢复了, 特别是在 1816 年巴黎科学院将它作为 1818 年年度竞赛奖的主题之后; 奥伯斯*[10] (Olbers) 拿它来引起高斯注目, 而高斯以他特有的谨慎回答说, 对于像这一类的问题他没有什么兴趣, 但是如果顺利的话, 它的解或许会产生一个他正在思考的高等算术在一个大范围上的副产品 (*einer grossen Erweiterung der höheren Arithmetik: Gau.* X-1,75;1816).

在其间, 苏菲 · 热尔曼*[11](Sophie Germain) 的天才早已引起了拉格朗日、勒让德以及高斯的注意. 她着手研究了费马的定理, 并得到了一些有价值的结果, 这些结果是建立在对于同余式的精巧的论证之上的 (参看譬如 H. M. Edwards,《*Fermat's last theorem*》, Springer 1977, p.64, 或者 P. Ribenboim,《*Thirteen lectures on Fermat's last theorem*》, Springer 1979, pp.53–55). 这些并不在我们讨论之列, 与我们有关的是在 1825 年狄利克雷与勒让德使用了无穷下降法到费马的指数为 5 的方程上.

属于费马的无穷下降法通常来说只不过有赖于如下的简单观察: 如果两个通常的整数的积 $\alpha\beta$ (分别地, 在代数数域的两个整数) 等于一个 m 次幂, 并且如果 α 和 β 的 g.c.d 只能取在一个已知的整数的 (理想的) 有限集合中, 那么 α 和 β 都是 m 次幂, 而它们被决定到差一个因子的程度, 并且这些因子也只在某

*[10]1758—1840, 德国天文学家, 以 "奥伯斯佯谬" 而知名.

*[11]1776—1831, 法国女数学家, 对于微分几何、数论特别对费马大定理颇有贡献.

个指定的有限集合中取值. 对于通常的整数这是显然的, 但对于代数数域, 如若理想类的个数的有限性和关于单位的狄利克雷定理想当然地成立, 那么上述结论也是对的. 在二次数域 $\mathbb{Q}(\sqrt{N})$ 的情形, 这可换成为一个关于具判别式 N 的二元二次型的一个陈述, 欧拉对于费马定理的证明 (参看第三章§14) 给出了一个典型的情形; 在那里的第一步在于将方程写成如下形式:

$$(x-y)(x-jy)(x-j^2y)=z^3,$$

其中 $j=(-1+\sqrt{-3})/2$ 是一个三次单位根, 然后将上面的原理用到左端的因子上, 如在第二章的附录 I 所表明的, 也如欧拉所知道的那样 (同上), 这可以容易地被以一个基于形式 X^2+3Y^2 的理论所代替.

在寻求处理费马方程 $x^p-y^p=z^p$, 其中 p 为 >3 的素数时, 自然是将 x^p-y^p 在 "分圆域" $\mathbb{Q}(\varepsilon)$ 中分解为线性因子, 其中 ε 是个 p 次单位根; 在 1801 年之后这是个非常有诱惑力的想法, 这是因为高斯已经在他的《*Disquisitiones*》的第 VII 节中发展了 $\mathbb{Q}(\varepsilon)$ 理论的代数方面; 1816 年在写信给奥伯斯时高斯清楚知道自己在想什么 (索引同上). 但是必须首先建立理想理论.

然而高斯自己已经表明了 x^p-y^p 在二次数域 $k=\mathbb{Q}(\sqrt{\pm p})$ 是如何分解因子的, 这里的符号是那个 $\pm p\equiv 1 \pmod 4$ 的符号; 如他所证, 这个域包含在 $\mathbb{Q}(\varepsilon)$ 之中, 由此推出在 $\mathbb{Q}$ 上不可约 (如高斯所证) 的多项式

$$F=\frac{x^p-y^p}{x-y}=x^{p-1}+x^{p-2}y+\cdots+y^{p-1},$$

分解为两个因子 $P+Q\sqrt{\pm p}$, $P-Q\sqrt{\pm p}$, 其中 P, Q 为两个对于 x, y 的 $(p-1)/2$ 次具半整系数的多项式; 这给出了恒等式

$$F=P^2\mp pQ^2,$$

故上面所叙述的原理在将费马方程写成

$$(x-y)(P+Q\sqrt{\pm p})(P-Q\sqrt{\pm p})=z^p$$

时可应用于它. 进一步, 尽管二次域 k 的理论仍可继续进行下去, 但取而代之人们可以, 甚至在勒让德仍然活着时就可以应用具判别式 $\pm p$ 的二元二次型的理论, 这从拉格朗日的著作和高斯的著作中都可了解到.

这正好是 1825 年刚刚满 20 岁的年轻的巴黎学生 L. 狄利克雷所做的事; 因为在那时的德国难于学到好的数学, 他来到巴黎学习. 自然他从第一个显著的情形 $p=5$ 着手; 这样做也会更容易些, 这是因为所需要的恒等式从欧拉那时起就已经知道了 (*Eu.*I-3,280 于 E449 中;1772), 这个等式就是

$$x^4+x^3y+x^2y^2+xy^3+y^4=\left(x^2+\frac{1}{2}xy+y^2\right)^2-5\left(\frac{1}{2}xy\right)^2;$$

欧拉是从关于形式 X^2-5Y^2 的一些部分结果中将它推导出来的 (参看前面的第三章§9).

在这第一次的努力中, 狄利克雷只取得了部分成功. 如果将该方程写成对称的形式 $x^5+y^5+z^5=0$, 其中的 x, y, z 没有公因子, 显然其中一个必为偶数而另两个均为奇数. 考虑同余式

$$x^5+y^5+z^5\equiv 0 \pmod{25},$$

也可看出这些未定量中必有一个 $\equiv 0 \pmod 5$ 而另两个均不能如此; 由前面提到的苏菲 · 热尔曼的定理可以推导出同样的结论, 只是要更精细些. 起初狄利克雷的处理 (用无穷下降法) 只能够用到这三个未知量中同一个是 2 的倍数和 5 的倍数的情形.

这正是已经超过七十岁的勒让德插手的地方. 在 1825 年 7 月将狄利克雷的文章提交给科学院后 (参看 *Dir.*I,3–13), 他只花了几个星期来处理剩余的情形, 所使用的技术与狄利克雷的没有太大的差别.

这或许是一座要登的高度适中的山峰, 狄利克雷已经几乎把他带到了山顶. 但是勒让德第一个到了那里. 他的整个证明写在 1825 年 9 月递交给科学院的一篇文章里, 并且作为对他的《*Essai*》的 "第二补充" 发表在科学院的《*Mémoires*》中; 在文中他适时地引述了 "苏菲 · 热尔曼小姐" 以及一个奇怪的 "L. Dieterich" (不是 Direchlet). 第二年狄利克雷返回了德国, 准备他的证明以便在新近创刊的克雷尔 (Crelle) 的杂志上发表, 它发表于 1828 年 (*Dir.*I,21–46); 在文中他放进了以前曾省略掉的情形. 勒让德则在他 1830 年的《*Théorie des Nombres*》的 II 卷中放进了他自己的证明版本而没有提及狄利克雷 (第 6 部分,§IV,pp.361–368). 那时他已使自己相信这份荣耀只单独是他的了吗? 倘若如此, 老年人应该得到原谅. 对于雅可比和阿贝尔他的表现是极其大度的, 对于他们在他另一个钟爱的课题, 椭圆函数理论上的发现不惜溢美之词. 至于狄利克雷, 他很快就已翱翔到勒让德梦想不到的高度了.

附录 I　三元二次型的哈塞 (Hasse) 原理

在这里对于形式我们理解为一些不定元 $X_1,\ X_2,\cdots,X_n$ 的任意 δ 次的整系数齐次多项式 F, 及系数在 $\mathbb{Z}$ 中. 无疑, 方程 $F=0$ 在 $\mathbb{Q}$ 中具有一个非平凡解, 即一个不全为 0 的有理数解, 当且仅当它在 $\mathbb{Z}$ 中有 "正常" 解, 即没有公因子的整数解. 另一方面, 同余式 $F\equiv 0 \pmod m$ 的解 $(x_1,x_2,\cdots,x_n)$ 是一个正常解是说, 如果整数 $x_1,x_2,\cdots,x_n$ 的 g.c.d.与 m 互素. 显然, 如果 m 和 m' 互素, 则 $F\equiv 0$ 具有一个模 mm' 的正常解当且仅当它模 m 和模 m' 都有这样的解.

设 G 为另一个这种形式, 其不定元为 $Y_1, Y_2, \cdots, Y_n$; 我们称方程 $F(X)=0$, $G(Y)=0$ 为等价是说如果存在系数在 $\mathbb{Z}$ 中具行列式 $D\neq 0$ 的线性变换将 F 变成 aG, 其中 $a\neq 0$; 这表明

$$F[S(Y)]=aG(Y).$$

于是变换 $T=aD\cdot S^{-1}$ 也具有整系数且有

$$G[T(X)]=a^{\delta-1}D^{\delta}F(X),$$

这表明 F 与 G 之间的关系是对称的; 由于它显然是自反与传递的, 故是在通常意义下的一个等价关系.

引理 1. 设 F, G 为使两个方程 $F=0$, $G=0$ 等价的形式; 设 p 是个素数. 于是同余式 $G\equiv 0 \pmod{p^{\mu}}$ 对于所有的 μ 有一个正常解当且仅当 $F\equiv 0$ 具有同样的性质.

记号如上, 设 p^{α} 为除尽 a 的最高次幂; 设 $x=(x_1,\cdots,x_n)$ 为 $F\equiv 0 \pmod{p^{\mu+\alpha}}$ 的一个正常解; 令 $y=T(x)$, 并记 p^{λ} 为除尽所有 y_i 的 p 的最高次幂. 令 $y'=p^{-\lambda}y$; 由于我们有

$$S(y')=p^{-\lambda}S(y)=p^{-\lambda}aDx,$$

并且因为 x 为正常解, 于是 p^{λ} 必除尽 aD. 现在我们有

$$aG(y')=F[S(y')]=(p^{-\lambda}aD)^{\delta}F(x);$$

由于右端为 $\equiv 0 \pmod{p^{\mu+\alpha}}$, $G(y')$ 因而必为 $\equiv 0 \pmod{p^{\mu}}$, 故 y' 为那个同余式的正常解.

运用 p- 进整数环的基本性质, 容易证明引理 1 中的假定条件 (分别地, 结论) 等于是说 $F=0$(分别地, $G=0$) 在 p- 进域 $\mathbb{Q}_p$ 中有一个非平凡解 (从而是一个正常的整数解). 在这样的注解后, 引理 1 成了显然的了.

在这里我们将特别关注非退化二次型; 这是写二次形式

$$F(X)=\sum_{i,j=1}^{n}a_{ij}X_iX_j,$$

其中行列式 $\det(a_{ij})$ 不为 0. 所说的哈塞–闵可夫斯基原理 (Hasse-Minkowski principle) 是说, 对于这样一个形式方程 $F=0$ 在 $\mathbb{Q}$ 中具有非平凡解 (从而有正常整数解) 当且仅当它在实数域 $\mathbb{R}$ 中有一个非平凡解, 并且对所有的整数 m 所

有同余式 $F \equiv 0 \pmod m$ 均有正常解. 这后一个条件完全等同于说方程 $F=0$ 对于每个素数 p 有一个 p- 进数的非平凡解[3]. 这个原理对于现代数论的价值由于它可以被推广到所有的代数数域而被大大地提高[4]. 如它实质上是由勒让德在 1785 年发现的那样, 对于三元情形成立一个稍强的形式:

定理 1. 设 $F(X,Y,Z)$ 为一个非退化三元二次型. 于是方程 $F=0$ 在 $\mathbb{Q}$ 有一个非平凡解当且仅当它在 $\mathbb{R}$ 有一个解并且对于每个奇素数 p 的每个幂 p^μ, 同余式 $F \equiv 0 \pmod{p^\mu}$ 有正常解.

当然这个条件是必要的; 只需证明它的逆. 经过一个初等的变换, 方程 $F=0$ 转换成了一个等价的方程

$$F(X,Y,Z)=aX^2+bY^2+cZ^2=0;$$

由于 F 为非退化, 这里的 a, b 和 c 不全为 0; 因为 $F=0$ 在实数域 $\mathbb{R}$ 有解, a, b 和 c 不具有完全一样的符号. 假定 F 满足我们定理的条件; 由于引理 1, 这表明每个等价于 $F=0$ 的方程 $G=0$ 满足同样的条件; 现在考虑解一个方程 $F=0$ 的拉格朗日方法, 该方法是我们在第二章 §14 中叙述过的; 在其中先用一个等价的方程 $Z^2=AX^2+BY^2$ 替换 $F=0$, 其中 A 和 B 不含平方因子且不全为负, 然后逐次地用相似的方程 $Z^2=MX^2+NY^2$ 替换, 每一个都等价于上一个, 直到到达一个方程, 在那里的 M 或者为 1 或者不满足任何同余式 $M \equiv m^2 \pmod{|N|}$. 在前一种情形, 这最后的一个方程从而原来的那个方程便有非平凡解. 我们来证明后一种情形不会出现, 因而定理得证.

事实上, 如果 M 不满足任何同余式 $M \equiv m^2 \pmod{|N|}$, 则由于 N 无平方因子, 它必定有一个因子 p 使得 M 不满足任何同余式 $M \equiv m^2 \pmod p$; 无疑 p 必为奇数. 考虑同余式

$$Z^2 \equiv NX^2+NY^2 \pmod{p^2};$$

如我们已看到过的, 从我们对于 F 的假设可知, 它有一个正常解 (x,y,z). 这里的 p 不能除尽 x; 因为, 如果能除尽, 它就会除尽 z; 那么 p^2 就会除尽 Ny^2, 但 N 无平方因子, 故 p 就会除尽 y, 从而 (x,y,z) 就不是正常的了. 现在取 x' 使得 $xx' \equiv 1 \pmod p$, 我们有 $M \equiv (x'z)^2 \pmod p$, 它与对 M 的假设相矛盾.

为了推导出勒让德对定理的原来的阐述, 我们需要一些引理.

[3]有一个基于从 p-进域观点的对二次型的初等处理的证明, 参看 J.-P.Serre 的《*Cours d'Arithmétique*》(有中译本), P.U.F. Paris 1970, 第 I–IV 章.

[4]至于哈塞发现他的 "原理" 的历史可参看 *Crelle J.*209 (1962), pp.3–4.

引理 2. 设 p 为素数. 如果 a, b 和 c 均与 p 互素, 则 $aX^2+bY^2+cZ^2\equiv 0 \pmod p$ 有一个正常解.

我们已经知道这是欧拉的一个定理; 其证明见前面的第三章§11.

引理 3. 设 p 为素数; 令 $F(X)=\sum_{i=1}^{n} a_iX_i^2$, 其中所有的 a_i 均与 p 互素. 假定同余式 $F(X)\equiv 0 \pmod{p^\mu}$ 有一个正常解, 其中当 $p\neq 2$ 时 $\mu\geq 1$, 而当 $p=2$ 则 $\mu\geq 3$. 于是, 同余式 $F(X)\equiv 0 \pmod{p^{\mu+1}}$ 有一个正常解.

设 $(x_1,\cdots,x_n)$ 为 $F(X)\equiv 0 \pmod{p^\mu}$ 的一个正常解, 于是我们可以写成 $F(X)=p^\mu r$, 且其中有一个 x_i, 譬如 x_1 与 p 互素. 令

$$y_1=x_1+p^\mu t,\quad \text{分别地, } y_1=x_1+2^{\mu-1}t$$

按照 $p\neq 2$ 或 $p=2$ 决定; 令 $y_i=x_i$, $i=2,\cdots,n$. 我们有

$$F(y)\equiv p^\mu(r+\delta a_1x_1t) \pmod{p^{\mu+1}},$$

其中如果 $p\neq 2$ 则 $\delta=2$, 如果 $p=2$ 则 $\delta=1$. 取 t 使得

如果 $F=0$ 在 $\mathbb{Q}$ 中有个非平凡解, 则它在 $\mathbb{Z}$ 中便有一个正常解 (x,y,z). 这里的 z 必定与 ab 互素; 因为如果, 譬如, p 是个除尽 z 和 a 的素数, 它则必除尽 by^2, 从而由于 b 与 a 互素, 故除尽 y; 于是 p^2 除尽 ax^2, 又因 a 无平方因子, 故 p 除尽 x, 故而 (x,y,z) 不是正常的了. 现在取 z' 使得 $zz'\equiv 1 \pmod{|ab|}$; 于是我们有 $-bc\equiv(byz')^2 \pmod{|a|}$ 以及 $-ca\equiv(axz')^2 \pmod{|b|}$; 对于 $-ab$ 的证明自然是相似的. 因此定理中的条件是必要的.

现假定它们满足定理的条件, 我们验证这些在定理 1 中也被满足. 设 p 为任一奇素数. 如果它不除尽 abc, 那么由引理 2, 同余式 $F\equiv 0 \pmod p$ 有一个正常解; 根据引理 3, 并对 μ 进行归纳, 这表明对于所有的 μ 具有模 p^μ 的这种解. 现设 p 为 abc 的一个因子, 譬如, c 的, 从而不是 ab 的. 由于 $-ab$ 是个模 $|c|$ 的平方剩余, 故我们可写成 $-ab\equiv m^2 \pmod p$. 于是 (m,a) 是同余式 $aX^2+bY^2\equiv 0 \pmod p$ 的一个正常解; 应用引理 3 并对 μ 进行归纳, 我们看到, 对于每个 μ, 这同一个同余式具有一个模 p^μ 的正常解 (x,y), 故而 $(x,y,0)$ 是 $F\equiv 0 \pmod{p^\mu}$ 的一个正常解. 证完.

推论. 设 N 为一无平方因子的整数且不是 0 或 -1; 设 p 为一奇素数且不除尽 N. 如果 p 是个模 $4|N|$ 的平方剩余, 则它可写成 a^2+Nb^2, 其中 a 和 b 为有理数.

将勒让德的定理用于方程 $X^2+NY^2=pZ^2$. 如果 p 是个模 N 的二次剩余, 而 $-N$ 是个模 p 的二次剩余, 则它有在 $\mathbb{Q}$ 中的非平凡解. 根据在第三章的附录 I 中所叙述的结果, 如果 p 是模 $4|N|$ 的平方剩余这两个条件都得到满足 (如果 p 为模 $|N|$ 的平方剩余且 $N\equiv -1 \pmod 4$ 也如此). 于是, 如果 (x,y,z) 是 $X^2+NY^2=pZ^2$ 的一个非平凡解, z 不能为 0, 故 $p=a^2+Nb^2$, 其中 $a=x/z$, $b=y/z$. 这是欧拉在 $N>0, p\equiv 1 \pmod{4N}$ 的情形下预言过的结果 (参看前面的第三章§9, 以及 *Corr.*I,605–606;1753).

最后, 由于勒让德将此定理用于二次互反律的一个证明 (仅部分成功), 似乎值得对于在这两个课题之间的关系做个简短的评述; 为此引进记号 $[F]_v$ 较为方便, 其中 F 是 $\mathbb{Z}$ 上的一个三元形式, 而 v 或是个素数或为 ∞. 如果 p 为素数, 我们令, 当方程 $F=0$ 在 $\mathbb{Q}_p$ 中有非平凡解时 $[F]_p=+1$, 或者等价地说, 如果同余式 $F\equiv 0 \pmod{p^\mu}$ 对所有的 μ 有正常解时为 $+1$; 否则令 $[F]_p=-1$. 我们令 $[F]_\infty=+1$ 或 -1 是按照 $F=0$ 在 $\mathbb{R}$ 中有无非平凡解决定. 对于 $F=Z^2-aX^2-bY^2$, $[F]_v$ 只不过是希尔伯特符号 $(a,b)_v$. 由于每个方程 $F=0$ 等价于后一个的那种类型的方程, 那么由引理 1, 2, 3 得到, 对于任意 F, 除有限多个素数 p 外我们有 $[F]_p=+1$.

将最一般形式的哈塞–闵可夫斯基原理应用于一个三元形式 F 时, 说 $F=0$

在 $\mathbb{Q}$ 中有一个非平凡解当且仅当 $[F]_\infty=+1$ 且对所有素数 p 有 $[F]_p=+1$. 另一方面定理 1 (或者等价地, 勒让德定理) 说对于 $F=0$ 在 $\mathbb{Q}$ 中有一个非平凡解只要对所有奇素数满足 $[F]_\infty=+1$ 和 $[F]_p=+1$ 就够了; 因此这些条件蕴含 $[F]_2=+1$.

这最后的条件实际是希尔伯特乘公式的一个特殊情形, 对于所有 $\mathbb{Z}$ 上的三元形式成立

$$[F]_\infty\cdot\prod_p[F]_p=1,$$

其中的乘积取所有的素数. 这实际上是说, 在左端的取 -1 的因子的个数必为偶数. 特别地, 如果除去可能 $[F]_2$ 外, 所有的因子全为 $+1$ 的话, 那么 $[F]_2$ 也必为 $+1$; 结合哈塞–闵可夫斯基原理, 这便给出了勒让德的结果.

希尔伯特的公式包含了二次互反律, 由此它这一回可由初等的想法推导出来 (参看 J.-P. Serre, 索引同上). 譬如将它应用到形式 $F=pX^2\pm qY^2-Z^2$, 其中 p 与 q 为其奇素数, 并且其中的符号由 $\pm q\equiv 1 \pmod 4$ 决定. 这里我们有 $[F]_\infty=+1$. 容易看出 $(0,0,1)$ 或者 $(2,1,1)$ 是 $F\equiv 0 \pmod 8$ 的正常解; 根据引理 3, 这给出了 $[F]_2=+1$. 引理 2 和引理 3 表明除了 $r=p,q$ 外 $[F]_r=+1$. 最后, 用像上面证明定理 2 那样的推理, 得到

$$[F]_p=\left(\frac{\pm q}{p}\right),\quad [F]_q=\left(\frac{p}{q}\right),$$

故而最后的这些符号或者都为 $+1$ 或者都为 -1. 我们在第三章附录 I 中已经看到过, 这不是别的, 就是二次互反律. 勒让德的定理蕴涵了乘积公式的一个特殊情形无论如何也说明他在把它运用到二次互反律是部分成功.

附录 II　关于正二元二次型的勒让德的证明

在对欧拉《代数学》的 “附件” 中, 拉格朗日提出了一个求 $|f(x,y)|$ 极小值的问题, 其中 f 是一个整系数的二元形式, 而 x, y 为不全为 0 的整数; 他使用了连分式的理论, 解决了对于定和不定的二次型的这个问题 (*Lag.*VII,61–74,Art.31–36=*Eu.*I-1,552–562).

在这同一个 “附件” 中, 他引进了 “拉格朗日简约” 方法 (参看前面的 §3), 后来则以他 1775 年整个的《*Recherches*》来讨论它. 实际上, 在这个课题与上面提到的极小问题之间存在着更加紧密的联系, 然而没有什么能显示拉格朗日曾留意到这种联系, 在定形式的情形似乎是勒让德在他的 1798 年的《*Essai*》中第一个指出了这一点. 他有赖于如下的观察.

为简便起见, 如果 $f=(a,b,c)$ 是一个二元二次型 (记号如上面的 §4 所解释的那样), 我们以 $\mu(f)$ 表示 $|f(x,y)|$ 在 x,y 为不全为 0 的整数时的极小值. 使 $\mu(f)=0$ 的是那些其判别式 b^2-4ac 为 0 或一个平方数的形式. 由于我们从此排除掉这种情形, 故 $\mu(f)$ 是个 >0 的整数.

引理 1. 设 f 为一二元二次型 (其判别式既非 0 也非平方数). 于是存在一个等价于 f 的形式 $F=(A,B,C)$, 使得 $A=\pm\mu(f)$, 并且 $|B|\le|A|\le|C|$.

取 (a,b) 使得 $|f(a,b)|=\mu(f)$. 如果我们有 $a=da'$, $b=db'$, 其中 $d>1$, 于是我们有

$$|f(a',b')|=|d^{-2}f(a,b)|<\mu(f).$$

因此 a 和 b 互素, 故 $f(a,b)$ 被 f 正常表示. 如在前面的 §4 所表明的, 于是有一个形式 $f'=(m,n,p)$ 等价于 f, 且其中 $m=f(a,b)=\pm\mu(f)$. 像在拉格朗日简约那样, 取 ν 使得 $-|m|\le n-2\nu m\le|m|$; 于是变换 $(X,Y)\mapsto(X-\nu Y,Y)$ 将 f' 变成了形式 $F(A,B,C)$, 其中 $A=m=\pm\mu(f)$, $|B|\le|A|$. 由于 C 由 F 正常表示, 故我们有 $|C|\ge\mu(f)$, 引理得证.

勒让德发现 (参看他的 1798 年的《*Essai*》, 第 I 部分,§VIII), 对于定形式, 存在对于引理 2 的某种逆命题. 下面所叙述的比勒让德的要更加准确:

引理 2. 设 $F=(A,B,C)$ 为一个二元二次型, 其中 $A>0$, $0\le B\le A\le C$. 于是, 如果 x, y 为整数, 我们则有 $F(x,y)>C$, 但以下情形例外: 对于 $x=0$, $y=\pm1$, 或者对于 $A=B$ 时的 $x=-y=\pm1$, 在这个情形我们有 $F(x,y)=C$, 或者, 可能有 $y=0$, 这时我们有 $F(x,0)=Ax^2$ (并且除非 $x=0$ 或者 ±1, 总有 $F(x,0)>A$; 又, 除非 $x=0$, 总有 $F(x,0)\ge A$).

设 $D=B^2-4AC$ 为 F 的判别式; 它 <0. 如果 $F(x,y)\le C$, 我们有

$$4AF(x,y)=(2Ax+By)^2+|D|y^2\le 4AC,$$

从而 $y^2\le 4AC|D|^{-1}$. 由于 $0\le B\le A\le C$, 我们有 $|D|\ge 3AC$; 这给出了 $y^2\le 4/3$, $y=0$ 或者 ±1. 如果 $y=\pm1$, 上面的不等式可重写为

$$(2Ax\pm B)^2+|D|-4AC=4A(Ax^2\pm Bx)\le 0,$$

即 $Ax^2\pm Bx\le 0$; 除非 $x=0$ 或者 $A=B$, $x=\mp1$, 否则它不成立, 在这些情形有 $F(x,y)=C$. 至于我们对 $y=0$ 情形的陈述是显然的.

引理 3. 设 $F=(A,B,C)$ 为满足引理 2 条件的一个形式. 于是 $\mu(F)=A$; 又, 如果 $C>A$, 我们有 $F(a,b)=A$ 当且仅当 $(a,b)=(\pm1,0)$; 如果 $C=A>B$,

我们有 $F(a,b)=A$ 当且仅当 $(a,b)=(\pm1,0)$ 或者 $(0,\pm1)$; 如果 $C=A=B$, 我们有 $F(a,b)=A$ 当且仅当 $(a,b)=(\pm1,0)$, $(0,\pm1)$ 或者 $(\pm1,\mp1)$.

这立即可由引理 2 推出.

定理. 设 $F=(A,B,C)$, $F'=(A',B',C')$ 为两个等价的形式, 它们都满足引理 2 的条件. 于是 $F=F'$.

由于 F 与 F' 等价, 我们可写成

$$F'(X,Y)=F(\alpha X+\beta Y,\gamma X+\delta Y),\ \alpha\delta-\beta\gamma=\pm1;$$

还有 $\mu(F)=\mu(F')$ 从而 $A=A'$; 这给出了 $F(\alpha,\gamma)=A$, 因此由引理 3 有 $\gamma=0$, $\alpha=\pm1$ 除非 $C=A$. 如果 $C=A$, 由引理 3, 存在 (a,b) 的四个或六个值使得 $F(a,b)=A$; 因此, 这对于 F' 也对, 故由同样的引理, 我们有 $C'=A'=A$; 由于 F 和 F' 具有相同的判别式, 并由于 B 和 B' 都 ≥ 0, 这给出了 $B=B'$, $F=F'$. 现在讨论 $C>A$, $\gamma=0$ 的情形; 于是我们有 $\alpha=\pm1$, $\delta=\pm1$. 这里我们有

$$B'=2A\alpha\beta+B\alpha\delta=\pm2A\beta\pm B,$$

从而 $2A\beta=\pm B\pm B'$. 因为 B 和 B' 都 ≥ 0 且 $\leq A$, 这表明 $B=B'$, 从而像上面那样有 $C=C'$, $F=F'$.

现在对于每一个形式 f, 拉格朗日简约过程产生了一个满足 $|B|\leq|A|$ 和 $|B|\leq|C|$ 的等价形式 $F=(A,B,C)$; 如果 f 为正定, A 和 C 必定都 >0, 而如果 f 为不定, 它们必定具有相反的符号, 这是因为 B^2-4AC 这时 >0 从而 $|AC|\geq B^2$. 由于显然形式 $(A,\pm B,C)$ 和 $(C,\pm B,A)$ 全都等价 (参看前面的 §4), 在正形式的每个拉格朗日类中必定至少有一个形式满足引理 2 的条件 $A>0$, $0\leq B\leq A\leq C$; 正如拉格朗日所发现的那样, 这是唯一的, 而上面这些引理在实质上构成了勒让德对这个结果的证明 (如他所说, 他是 "*par une méthode particulière* (用一个特别的方法)" 得到的:《*Essai*》,p.xii).

至于确定一个不定形式 f 的 $\mu(f)$, 引理 1 说存在一个等价于 f 的形式 $F=(A,B,C)$, 它是在 "拉格朗日意义下" 简约的, 对它有 $\mu(f)=|A|$; 因此这个问题可用构造这样的形式来解决. 拉格朗日对此的方法现在就要在附录 III 中叙述.

附录 III 拉格朗日关于不定二元二次型的一个证明

为方便起见, 在前面 §4 引进的记号之外我们再采用矩阵的记号, 因此我们

记由 §4 中 (2) 给出的变换为

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}.$$

我们也记 §4 中由 (1) 给出的形式为 $f\circ S$, 即在变换 S 下形式 f 的形变, 以 $\mathscr{G}$ 记群 $GL(2,\mathbb{Z})$ 中具整系数 α, β, γ, δ 的变换 S 使得 $\det S=\pm 1$. 以乘法记群 $\mathscr{G}$ 的运算; 因此, 对于 $\mathscr{G}$ 中的 S 和 T, ST 代表变换

$$(x,y)\mapsto ST(x,y)=S[T(x,y)];$$

于是, 对于形式 f, 我们有 $f\circ ST=(f\circ S)\circ T$. 当然这些记号对拉格朗日来说是陌生的, 它们只是在十九世纪和二十世纪才发展起来的.

在这种语言的表达下, 拉格朗日的第一个观察到的是如下的命题.

引理 1. $\mathscr{G}$ 中的每个 $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ 在右乘和左乘形如 $\begin{pmatrix}\pm 1 & 0\\ 0 & \pm 1\end{pmatrix}$ 下变成一个相似的矩阵, 但 α, β, γ, δ 均 ≥ 0.

对它右乘这些变换中的一个可将它变成 $\alpha>0$, $\beta>0$ 的矩阵 (如果两个都不为 0) 否则变成一个 α 和 β 都 ≥ 0 的, 而 γ, δ 不具相反的符号 (如果 α 或 β 为 0). 在前一种情形, 关系式 $\alpha\beta-\gamma\delta=\pm 1$ 表明 γ, δ 不具相反的符号. 然后以 $\begin{pmatrix}1 & 0\\ 0 & \pm 1\end{pmatrix}$ 之一左乘就得到我们所要的结果.

我们以 $\mathscr{G}_+$ 记 $\mathscr{G}$ 中那些 α, β, γ, δ 全 ≥ 0 的变换; 这是一个半群, 即在 $\mathscr{G}_+$ 中变换的乘积仍在 $\mathscr{G}_+$ 中. 对于这些, 拉格朗日在实质上证明了它们全都可以通过 $(x,y)\mapsto(y,x)$ 和 $(x,y)\mapsto(x,y+\mu x)$, $\mu>0$ 逐次的变换得到. 如果在矩阵记号下我们令

$$J=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad T=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix},$$

则这些便是变换 J, T^μ; 我们有

$$T^\mu=\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix},\quad JT^\mu=\begin{pmatrix}\mu & 1\\ 1 & 0\end{pmatrix},\quad J^2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

用这些记号可以将拉格朗日的结果叙述于后:

定理 1. $\mathscr{G}_+$ 中的每一个变换均可表达为变换 J 和 T^μ 的乘积, 其中 $\mu>0$.

取 $\mathscr{G}_+$ 中的 $S=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$; 如果 $\alpha<\beta$, 将 S 换作 SJ 之后可设 $\alpha\geq\beta$. 实质上, 拉格朗日此后便对 β 进行了归纳; 按照他的步骤, 我们首先考虑 $\beta>1$ 的

情形. 由于 $\alpha \geq \beta$, 我们可写成 $\alpha = \mu\beta + \rho$, 其中 $0 \leq \rho < \beta$, 这完全像求 α 和 β 的 g.c.d. 的欧几里得辗转相除的过程, 或者是构造 α/β 的连分式的过程. 这里, 由于 $\alpha\delta - \beta\gamma = \pm 1$, α 与 β 互素, 故 $\rho > 0$. 于是, 令

$$\sigma = \gamma - \mu\delta,\ S' = \begin{pmatrix} \beta & \rho \\ \delta & \sigma \end{pmatrix},$$

我们便有 $S = S'JT^{\mu}$. 由于 S, J 以及 T^{μ} 均在 $\mathscr{G}$ 中, 故 S' 也在其中; 因此我们有

$$\det S' = \beta\sigma - \rho\delta = \pm 1.$$

这表明 $\sigma \geq 0$, 不然的话我们就会有

$$\beta\sigma - \rho\delta \leq \beta\sigma \leq -\beta < -1.$$

所以 S' 便在 $\mathscr{G}_+$ 之中. 于是我们像拉格朗日那样, 当 $\rho > 1$ 时在 S' 做同样的运算, 或者等价地, 假若 $\beta = 1$ 和 $\beta = 0$ 已首先处理过了, 则在 S' 上应用归纳假定.

在情形 $\beta = 1$, 令 $\alpha = \mu\beta + \rho$, 其中如果 $\alpha\delta - \beta\gamma = -1$, 则令 $\mu = \alpha$ 及 $\rho = 0$, 如果 $\alpha\delta - \beta\gamma = 1$, 则令 $\mu = \alpha - 1$, $\rho = 1$ (在这个情形 α 和 δ 必定 ≥ 1; 拉格朗日对此格外地小心谨慎, 他觉得这种情形不会出现, 并甚至给出了一个谬误的推理来证明它: *Lag.*III,733,8–9 行). 在这两种情形, 还是取 $\sigma = \gamma - \mu\delta$, 即 $\sigma = \gamma - \alpha\delta = 1$, 分别地, $\sigma = \gamma - (\alpha - 1)\delta = \delta - 1$. 于是像前面那样我们得到 $S = S'JT^{\mu}$, 其中

$$S' = T^{\delta}, \quad \text{分别地},\ S' = \begin{pmatrix} 1 & 1 \\ \delta & \delta - 1 \end{pmatrix};$$

在后面的这个情形中, 在 S' 上重复这个步骤我们得到 $S' = Y^{\delta-1}JT$, 这便完成了对 $\beta = 1$ 的证明. 如果 $\beta = 0$, 我们必有 $\alpha = \delta = 1$ 从而 $S = T^{\gamma}$.

对于 $\mathscr{G}_+$ 中的每个 S, 以上的步骤给出了一个表达式

$$S = T^{\mu_0}JT^{\mu_1}JT^{\mu_2}\cdots JT^{\mu_m},$$

其中所有 $\mu_i \geq 0$, 并且除去可能的第一个或最后一个外全都 > 0, 而对于 $m > 0$, μ_i 决定了 α/β 的一个连分式

$$\frac{\alpha}{\beta} = \mu_m + 1/(\mu_{m-1} + 1/\cdots + 1/(\mu_2 + 1/\mu_1)\cdots).$$

可以容易证明对于 S 的上述表达式是唯一的, 但拉格朗日并没有考虑这一点.

我们现在来叙述拉格朗日将定理 1 应用到不定二元二次型的情形; 记住我们已经排除了那些判别式为 0 或是平方数的形式.

将拉格朗日简约过程 (第四章§4; 参看第三章的 §9) 应用到一个已知的形式导出了一个在 "拉格朗日意义" 下的简约形式 (A,B,C), 即它满足 $|B|\le|A|,\le|C|$, 故而 $B^2\le|AC|$. 于是 B^2-4AC 具有 $-4AC$ 的符号, 那么, 如果像我们在此假定的那样, 它 >0, 则 A 和 C 必具有相反的符号, 即 $AC<0$. 为了方便起见, 我们称一个形式 $f=(a,b,c)$ 为 *弱简约的* 是说它满足 $ac<0$; 这等于是说多项式 $f(X,1)=aX^2+bX+c$ 有两个符号相反的实根. 显见的是, 对于给定的判别式只有有限个弱简约形式. 如果 $f=(a,b,c)$ 为弱简约, 则 $f\circ J=(c,b,a)$ 也是.

为了把拉格朗日对他的问题的处理看得清楚一些, 还是有必要对那些是 $f(X,1)$ 有一个 >1 的正根和一个 >-1 的负根的形式 f 给个名字; 我们称它们为*强简约的*. 这个概念确实已暗含在拉格朗日的计算中了, 也含在他对佩尔方程的解中以及在对二次无理数的连分式的处理中 (参看前面的 §2(B)), 这两个课题与当前这一个紧密相关. 出于同样的理由, 它也已经在我们第二章 §13 对佩尔方程的讨论中出现过 (在 "简约形式" 的名字下). 在《*Disquisitiones*》中高斯引进了一个紧密相关的概念, 也叫做 "简约形式" (*Disq.*Art.183); 或许他仅仅是把它从拉格朗日的计算中剥离出来并用于自己的目的.

拉格朗日的问题是决定什么时候两个在他的意义下的简约方程是等价的. 他的解答依赖于下面的一些引理所表达的事实. 像通常那样, 如果 ξ 为任一实数, 我们以 $[\xi]$ 表示由 $\mu\le\xi<\mu+1$ 所决定的整数 μ, 即 $\le\xi$ 的最大整数.

引理 2. 设 f 为一弱简约形式; 设 ξ 为 $f(X,1)$ 的那个正根. 那么, 对于 $\mu>0$, 形式 $f'=f\circ JT^\mu$ 为弱简约的当且仅当 $\mu\le\xi$, 为强简约当且仅当 $\mu=[\xi]$; 而形式 $f''=f\circ JT^\mu J$ 总不是强简约的.

令 $f(1,0)=a$, 并以 $-\eta$ 记 $f(X,1)$ 的那个负根. 于是

$$f'(X,Y)=f(\mu X+Y,X)=a[Y+(\eta+\mu)X]\cdot[Y-(\xi-\mu)X].$$

这是弱简约的当且仅当 $\xi-\mu>0$. $f'(X,1)$ 的根为

$$\xi'=\frac{1}{\xi-\mu},\quad -\eta'=\frac{-1}{\eta+\mu}.$$

如果 $\mu>0$, 则 $\eta'>0$ 且 <1; 至于 ξ', 它 >1 当且仅当 $0<\xi-\mu<1$, 即 $\mu=[\xi]$. 最后, $f''(X,1)$ 的根为 $\xi-\mu$ 和 $-\eta-\mu$, 且后者 <-1.

由此推出, 每个弱简约形式等价于一个强简约形式, 就是说, 如果 $f(X,1)$ 的正根 $\xi>1$, 等价于对 $\mu=[\xi]$ 的 $f\circ JT^\mu$, 而如果 $\xi<1$, 则等价于对于

$\mu = [1/\xi]$ 的 $(f \circ J) \circ JT^\mu = f \circ T^\mu$, 这是因为在后一种情形我们可以将引理 2 用到 $f \circ J$ 上. 因为每个形式等价于在拉格朗日意义下的简约形式, 并且每个在那个意义下为简约的不定形式是弱简约的, 这表明在每个不定形式的拉格朗日类中至少有一个强简约形式. 有鉴于此以及引理 2, 拉格朗日的问题等于是求等价于所给不定形式的所有强简约形式. 对此的关键包含在下面的引理中 (参看 *Lag.*III,730–732):

引理 3. 设 S' 为 $\mathscr{G}_+$ 中一个变换; 令 $S = S'JT^\mu$, 其中 $\mu > 0$. 设 f 为一弱简约形式; 设 $F' = f \circ S'$ 以及 $F = f \circ S$ 为它分别在 S' 和 S 下的形变. 于是, 如果 F 为弱简约的, 则 F' 也是.

令 $f(1,0) = a$; 设 ξ, $-\eta$ 分别为 $f(X,1)$ 的正和负的根; 我们有

$$f(X,Y) = a(X+\eta Y)(X-\xi Y).$$

如定理 1 的证明那样, 设 S' 由 $S' = \begin{pmatrix} \beta & \rho \\ \delta & \sigma \end{pmatrix}$ 给出, 故我们有 $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, 其中 $\alpha = \mu\beta + \rho$, $\gamma = \mu\delta + \sigma$. 令 $F = (A,B,C)$, $F' = (A',B',C')$. 我们有

$$\begin{aligned} A &= f(\alpha,\gamma) = a(\alpha+\eta\gamma)(\alpha-\xi\gamma), \\ C = A' &= f(\beta,\delta) = a(\beta+\eta\delta)(\beta-\xi\delta), \\ C' &= f(\rho,\sigma) = a(\rho+\eta\sigma)(\rho-\xi\sigma). \end{aligned}$$

令

$$\theta = \alpha - \xi\gamma, \quad \zeta = \beta - \xi\delta, \quad \omega = \rho - \xi\sigma.$$

说 $AC < 0$ 等于是说 θ 和 ζ 具相反的符号; 我们必须证明, 当此条件满足时, ζ 与 ω 也具有相反的符号, 或者等同于 ω 具有 θ 的符号. 这立即由 $\omega = \theta - \mu\zeta$ 推出.

引理 4. 设 f 为弱简约形式; 设 ξ 为 $f(X,1)$ 的正根; 又设 μ, ν 为全 > 0 的整数; 令 $f' = f \circ JT^\mu$, $f'' = f' \circ JT^\nu$. 于是, 如果 f'' 为弱简约, 则 f' 为强简约, $\xi > 1$, 并且 $\mu = [\xi]$.

将引理 3 用于 $S' = JT^\mu$, $S = S'JY^\nu$ 以及 f, 我们看出 f' 必定是弱简约的. 如在引理 2 的证明中的那样, $f'(X,1)$ 的正根为 $\xi' = 1/(\xi - \mu)$. 现将引理 2 应用到 f' 和 f'' 上; 它表明我们有 $\xi' > \nu$; 由于 $\nu \geq 1$, 这给出了 $0 < \xi - \mu < 1$, 即 $\mu = [\xi]$; 由引理 2, 这表明 f' 为强简约.

引理 5. 设 $\mu_1, \mu_2, \cdots, \mu_m$ 为全 >0 的整数; 对于 $1 \le i \le m$, 令

$$S_i = JT^{\mu_1}JT^{\mu_2}\cdots JT^{\mu_m}.$$

设 f_0 为一个弱简约形式; 对于 $1 \le i \le m$, 令 $f_i = f_0 \circ S_i$, 并假定 f_m 为弱简约. 于是 $f_1, f_2, \cdots, f_{m-1}$ 为强简约; 另外, 如果 ξ_i 是 $f_i(X,1)$ 的正根, 对于 $1 \le i \le m$ 我们有 $[\xi_{i-1}] = \mu_i$, 且 ξ_0 由连分式

$$\xi_0 = \mu_1 + 1/(\mu_2 + 1/\cdots + 1/(\mu_i + 1/\xi_i)\cdots)$$

给出.

由引理 3 得到, f_{m-1} 为弱简约, 于是, 逐步地用对 j 的归纳得到了 f_{m-j} 为弱简约, 其中 $j = 2, 3, \cdots, m-1$. 引理中的断言于是由将引理 4 应用于 f_{i-1}, f_i, f_{i+1}, $1 \le i \le m-1$ 得到.

设 f 为一个弱简约形式, 使得 $f(X,1)$ 的正根 $\xi > 1$; 于是, 对于 $\mu = [\xi]$, 我们称强简约形式 $f' = f \circ JT^{\mu}$ 是个 f 的拉格朗日变换, 或者更准确地, f 的拉格朗日第一变换; 因而它由

$$f'(X,Y) = f(\mu X + Y, X)$$

给出. 那么可以迭代这个步骤, 即应用于 f', 然后应用于 f' 的变换 f'', 等等; 因此在引理 5 中, 形式 $f_1, f_2, \cdots, f_{m-1}$ 是 f_0 的前面 $m-1$ 个逐次的拉格朗日变换. 例如, 在第二章的 §8 中, 形式 $(-1)^i F_{i-1}$, $i = 1, 2, 3, \cdots$ 就是弱简约形式 $X^2 - NY^2$ 的逐次的拉格朗日变换.

从这些事实拉格朗日推导出他的问题的解答, 它以 "在拉格朗日意义下的简约" 形式来阐述. 如上所注意到的, 它也同样可以用 "强简约形式" 来阐述 (而且更简洁, 更优美); 它包含在下面的定理中:

定理 2. 设 $f = (a, b, c)$, $F = (A, B, C)$ 为两个等价的不定形式, 它们全为强简约的; 令 $f^* = (c, -b, a)$, $F^* = (C, -B, A)$. 于是, F 或者 F^* 是 f 或者 f^* 的逐次的拉格朗日变换之一.

设 S 为 $\mathscr{G}$ 中的一个变换, 使得 $F = f \circ S$. 首先考虑 S 在 $\mathscr{G}_+$ 的情形. 于是由定理 1 知, 我们可以写成

$$S = T^{\mu_0}JT^{\mu_1}J\cdots JT^{\mu_m},$$

其中所有的 $\mu_i > 0$, 但可能要除去第一个和最后一个, 它们 ≥ 0. 如果 $\mu_0 = 0$, $\mu_m > 0$, 引理 5 连同引理 2, 表明 F 是第 m 个 f 的拉格朗日变换. 如果 μ_m

为 0, 我们则可写成

$$SJ = S'JT^{\mu_{m-1}},$$

其中如果 $m=1$ 则 $S'=J$, 但无论如何 S' 总在 $\mathscr{G}_+$ 中. 这给出了

$$F \circ J = f \circ S'JT^{\mu_{m-1}};$$

这里, 由于 f 和 $F \circ J$ 为弱简约, 我们可将引理 3 用于 f, $f \circ S'$ 和 $F \circ J$; 它表明 $f \circ S'$ 必为弱简约. 于是将引理 2 应用于 $f \circ S'$ 表明形式

$$F = (f \circ S') \circ JT^{\mu_{m-1}}J,$$

不会是强简约, 这与我们的假定矛盾; 因此 $\mu_m > 0$. 现在我们来证明 μ_0 必为 0. 事实上, 如果 $\mu_0 > 0$, 我们则可写成 $F = f' \circ S_0$, 其中 $f' = f \circ J$, 而 S_0 由

$$S_0 = JT^{\mu_0}J \cdots JT^{\mu_m}$$

给出; 因为 f' 为弱简约, 引理 5 表明 $f' \circ JT^{\mu_0}$ 当 $m \geq 1$ 时为强简约; 如果 $m=0$, 由假定条件这同样是对的. 那么引理 2 表明 $f'(X,1)$ 的正根必 $> \mu_0$; 但是这是不可能的, 这是因为如果 ξ 是 $f(X,1)$ 的正根, 那么这个根便是 $1/\xi$, 并因为 f 为强简约我们有 $\xi > 1$. 对于 S 在 $\mathscr{G}_+$, 这证明了我们的定理.

如果 S 不在 $\mathscr{G}_+$ 中, 则由引理 1, 它可写成 $ES'E'$, 其中 S' 在 $\mathscr{G}_+$ 中, E, E' 为 $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. 记 H 为变换 $(x,y) \mapsto (y,-x)$, 即其矩阵形式为

$$H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

我们有

$$H^2 = -I_2, \quad HJ = -JH = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

其中 I_2 是 $\mathscr{G}$ 中的单位元. 现在变换 E, E' 中的每一个可以被表达为或者 $\pm I_2$, 或者 $\pm HJ = \mp JH$. 因此引理 1 表明 $\mathscr{G}$ 中每个变换 S 表达为形式 $\pm S'$, $\pm HS'$, $\pm S'H$, $\pm HS'H$ 中的一个, 其中 S' 在 $\mathscr{G}_+$ 中. 从而, 如果 $F = f \circ S$, 则形式 F 和 $F^* = F \circ H$ 中的一个是在 $\mathscr{G}_+$ 中的 S' 下或者是 f 或者是 $f^* = f \circ H$ 的变换. 根据以上已证明的便完成了对我们定理的证明. 还应该注意到, 如果 $f = (a,b,c)$ 为弱 (分别地, 强) 简约, 那么 $f^* = f \circ H = (c,-b,a)$ 也是.

拉格朗日对于一个实质上等价于定理 2 的一个结果 (但以在 "拉格朗日意义下简约" 的形式表达) 加上了进一步的注释. 由于对于具有给定判别式的简

约形式只有有限多个, 因此对于任意给定形式 f 的拉格朗日变换的序列中某个形式必定出现两次, 故这样一个序列一定是周期的, 至少从某一项起往后是如此的. 所以如拉格朗日看到的 (*Lag.*III,740–741), 该序列在那一项往后便没有必要继续下去了, 从而这个过程是有限步的.

但是从解佩尔方程我们得到提示 (*Lag.*II,494–496; 参看同前的 pp.429–443 以及 603–615, 还有前面的第二章 §8), 我们可以往前再走一步. 设 f_0 为一强简约形式; 设 f_1, f_2, 等为它的拉格朗日变换序列, 其中像前面那样, $f_i = f_{i-1} \circ JT^{\mu_i}$; 令 ξ_i 为 $f_i(X,1)$ 的正根; 由引理 5, 我们有

$$\mu_{i+1} = [\xi_i],\ \xi_{i+1} = \frac{1}{\xi_i - \mu_{i+1}},\ \xi_0 = \mu_1 + 1/(\mu_2 + 1/\cdots);$$

μ_1, $\mu_2, \cdots$ 等是出现在 ξ_0 的连分式中逐次的整数; 因为序列 (f_i) 至少从某一项开始往后是周期的, 故序列 (μ_i) 亦如此. 现在令 $f_i^* = f_i \circ H$. 根据这个容易验证的恒等式

$$H(JT^\mu)^{-1}H^{-1} = -JT^\mu,$$

我们有

$$f_{i-1}^* = f_i^* \circ JT^{\mu_i}.$$

由于所有的 f_i^* 为强简约, 这表明 f_{i-1}^*, $f_{i-2}^*, \cdots$ 等为 f_i^* 的逐次拉格朗日变换. 现在, 因为这些形式 f_i 必自身重复, 故可假定对于某个 j 和某个 $n > 0$ 有 $f_{j+n} = f_j$. 于是有 $f_{n+j}^* = f_j^*$, 从而 $f_{j+n-1}^* = f_{j-1}^*$, 等等, 并且最终 $f_n^* = f_0^*$, 它蕴涵了对所有 $i > 0$, $f_n = f_0$, $f_{n+i} = f_i$, $\mu_{n+i} = \mu_i$. 这样一来, 由于我们有 $f_n^* = f_0^*$, f_0^* 的逐次拉格朗日变换就是 f_{n-1}^*, $f_{n-2}^*, \cdots, f_1^*$ 以及再次的 f_0^*. 因此定理 2 可以换成如下更准确的陈述: 等价于 f_0 的强简约形式为 $f_1, f_2, \cdots, f_{n-1}$ 以及 f_0^*, $f_1^*, \cdots, f_{n-1}^*$, 当然假如它们不同于 $f_0, f_1, \cdots, f_{n-1}$ 的话.

补充参考文献

ĀRYABHAṬA: cf. K. Elfering.

L. Aubry, Solution de quelques questions d'analyse indéterminée, Sphinx-Œdipe, 7[e] année (1912), pp. 81–84.

BACHET: Claude Bachet, sieur de Méziriac, Problèmes plaisants et delectables qui se font par les nombres, avec leur demonstration, Lyon, Pierre Rigaud 1612; 2[e] éd., 1624.

JAC. BERNOULLI: Jacobi Bernoulli ... Ars Conjectandi, Opus Posthumum ... Basileae 1713.

BOMBELLI: (a) L'Algebra, Opera di Rafael Bombelli da Bologna, divisa in tre libri ... In Bologna, per Giovanni Rossi 1572, con licenza de' Superiori; (b) Rafael Bombelli da Bologna, L'Algebra, Prima edizione integrale, Feltrinelli, Milano 1966.

S. Chowla and W. E. Briggs, On discriminants of binary quadratic forms with a single class in each genus, Can. J. of Math. 6 (1954) 463–470.

B. Datta and A. N. Singh, History of Hindu Mathematics, A Source Book, 2 vol., Lahore 1935–1938 (vol.II, Algebra).

DIOPHANTUS: (a) Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Nunc primum Græcè et Latinè editi, atque absolutissimis Commentariis illustrati. Auctore Claudio Gaspare Bacheto Meziriaco Sebusiano V.C., Lutetiae Parisiorum, Sumptibus Hieronymi Drouart, via

Jacobæa, Sub Scuto Solari M.DC.XXI Cum Privilegio Regis; (b) Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Com Commentariis C.G.Bacheti V.C. et observationibus D.P. de Fermat Senatoris Tolosani. Accessit Doctrinae Analyticae inuentum nouum, collectum ex varijs eiusdem D. de Fermat Epistolis. Tolosæ, Excudebat Bernardus Bosc, è Regione Collegij Societatis Iesu, M.DC.LXX.

DIRICHLET-DEDEKIND: Vorlesungen über Zahlentheorie von P.G.Lejeune Dirichlet, herausgegeben und mit Zusätzen versehen von R. Dedekind, 4[te] Aufl., Braunschweig, F.Vieweg und Sohn, 1894.

K. Elfering, Die Mathematik des Āryabhaṭa I, Text, Übersetzung aus dem Sanskrit und Kommentar, W. Fink Verlag, München 1975.

ENCYCLOPÉDIE, ou Dictionnaire raisonné des Sciences, des Arts et des Métiers, par une Société de Gens de Lettres. Mis en ordre et publié par M. Diderot, de l'Académie Royale des Sciences et des Belles-Lettres de Prusse; et quant à la Partie Mathématique, par M. d'Alembert, de l'Académie Royale des Sciences de Paris, de celle de Prusse, et de la Société Royale de Londres (Tome Quatrième, à Paris, MDCCLIV, avec approbation et privilège du Roy).

G. Eneström: (a) Der Briefwechsel zwischen Leonhard Euler und Johann I. Bernoulli, Bibl. Math. 4 (1903) 344–388, 5 (1904) 248–291, 6 (1905) 16–87; Der Briefwechsel zwischen Leonhard Euler und Daniel Bernoulli, ibid. 7 (1906–07) 126–156; Zur Geschichte der unendlichen Reihen um die Mitte des siebzehnten Jahrhunderts, ibid. 12 (1911–12) 135–148; (b) Verzeichnis der Schriften Leonhard Eulers, Jahresb. d.D.M.V. (Ergänzungsband IV), 1910–1913.

A. Enneper, Elliptische Functionen, Theorie und Geschichte, Halle 1876.

EULER: Leonhardi Euleri Opera Postuma Mathematica et Physica, Anno 1844 detecta ... edd. P.-H.Fuss et Nic. Fuss, Petropoli 1862 (Reprint, Kraus 1969).

L. Euler und Chr. Goldbach, Briefwechsel, edd. A.P.Juškevič und E. Winter, Berlin 1965.

FAGNANO: Produzioni Matematiche del Conte Giulio Carlo di Fagnano, Marchese de' Toschi ... In Pesaro, l'anno del Giubileo M.DCC.L ... con licenza de' Superiori (2 vol. = *Fag.*I–II).

FERMAT: Varia Cpera Mathematica D.Petri de Fermat Senatoris Tolosani ... Tolosae, Apud Joannem Pech ... juxta Collegium PP. Societatis Jesu M.DC.LXXIX.

FRENICLE: Traité des Triangles Rectangles en nombres ("par M. Frenicle de Bessy", in Mémoires de l'Academie Royale des Sciences, tome V, 1729,pp. 127–

206; "la première Partie du Traité ... avoit été imprimée dès l'année 1676, in douze, et réimprimée avec la seconde en 1677 au Louvre").

E. GALOIS, Sur la théorie des nombres, Bull. de Férussac XIII (1830), p. 428–436 = Œuvres mathématiques d'Évariste Galois, Paris Gauthier-Villars 1897, pp. 15–23.

A. Genocchi, Démonstration d'un théorème de Fermat, Nouv. Ann. de Math. (III) 2 (1883) 306–310.

A. GIRARD: Les Œuvres Mathématiques de Simon Stevin ... reveu, corrigé et augmenté par Albert Girard, Leyde, Elzevir 1634.

F. Grube, Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen, Zeitschr. f. Math. u. Physik 19 (1874) 492–519.

H. Hasse, Kurt Hensels entscheidender Anstoss zur Entdeckung des Lokal-Global-Prinzips, Crelles J. 209 (1962) 3–4.

J. L. Heiberg und H. G. Zeuthen, Einige griechische Aufgaben der unbestimmten Analytik, Bibl. Math. 8 (1907–1908) 118–134.

HURWITZ: Mathematische Werke von Adolf Hurwitz, Basel, Birkhäuser, 2 vol. 1932–1933.

J. Itard, (a) Arithmétique et Théorie des Nombres, P.U.F. Paris 1973; (b) Sur la date à attribuer à une lettre de Pierre Fermat, Rev. Hist. des Sc. 2 (1948) 95–98.

W. Knorr, Archimedes and the measurement of the Circle, A new interpretation, Arch.Hist.ex.Sc. 15 (1975) 115–140.

J. LANDEN, An investigation of a general theorem for finding the length of any arc of any conic hyperbola, by means of two elliptic arcs, with some other new and useful theorems deduced therefrom, Phil. Trans. LXV (1775) 283–289.

LEGENDRE: (a) Recherches d'Analyse Indéterminée, Par M. Le Gendre, in: Histoire de l'Académie Royale des Sciences, Année M.DCCLXXXV, avec les Mémoires de Mathématique et de Physique pour la même Année ... A Paris, de l'Imprimerie Royale M.DCCLXXXVIII, pp. 465–559; (b) Adrien-Marie Le Gendre, Mémoire sur les Transcendantes elliptiques ... lu à la ci-devant Académie des Sciences en 1792, A Paris, l'an deuxième de la République; (c) Essai sur la Théorie des Nombres; par A.M. Le Gendre, de l'Institut National, A Paris, Chez Duprat, Libraire pour les Mathématiques, quai des Augustins, An VI; (d) Adrien-Marie Legendre, Théorie des Nombres, troisième édition. Paris, Firmin-Didot, 2 vol. 1830.

MACLAURIN: Colin MacLaurin, A treatise of fluxions, Edinburgh, 2 vol. 1742.

D.Mahnke, Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung, Bibl. Math. 13 (1912–1913) 29–61.

A. de MOIVRE: (a) The Doctrine of Chances, London 1718; (b) Miscellanea Analytica de Seriebus et Quadraturis ... (1 vol. + Supplementum) Londini 1730.

O. Neugebauer and A. Sachs, Mathematical cuneiform texts, New Haven 1945.

B. PASCAL, Œuvres Complètes, éd. J. Chevalier, Bibl. de la Plélade, Gallimard 1954 (pp. 97–108: Traité du triangle arithmétique; pp. 194–208: Histoire de la roulette).

K. Shukla, Ācārya Jayadeva the mathematician, Ganita 5 (1954) 1–20.

J. Steinig, On Euler's idoneal numbers, Elem.d.Math. 21 (1966) 73–88.

THEON: Theonis Smyrnaei ... Expositio rerum mathematicarum ad legendum Platonem utilium, rec. E. Hiller, Lipsiae, Teubner 1878 (and: Theon of Smyrna, Mathematics useful for understanding Plato, transl. by R. and D. Lawlor ... San Diego, Wizards Bookshelf 1979).

译后记

由于作者所处的社会和人文环境与我们所处的有较大的差异, 他所耳熟能详的人物、事件在书中往往一带而过, 但许多对我们是陌生的或朦胧的，有时可能会形成阅读的难点; 所以我尝试在译文中加了一些注解: 除了书中已有评说的外, 著名的人物和与后文无大关系的人物不予加注, 当然我找不到资料的也无从加注. 人名的翻译则沿用通用的或别人用过的, 一些无关紧要的人的名字甚至也没有做汉语音译; 名字终究不过是个符号而已. 限于水平, 也只能做到这一步了. 还望翻阅此译本的诸君能不吝指正.

作者是位公认的二十世纪的伟大数学家, 很高兴王元先生能慷慨答允为此做些介绍. 就该书本身而言, 我在译完全书后, 对作者不仅做数学而且做其他学问的严谨态度不由不敬佩有加: 几乎有断言就有考证, 并没有利用自己的崇高身份妄下结论, 或者天马行空般的指东道西, 发表没有根据的议论; 我想这或许应该是对待数学史研究的正确态度吧.

译者

2009 年 9 月 15 日

又, 接王元先生来函, 谈及写本译本介绍问题, 十分谦虚地解释了不能践诺的原因. 征得王元先生的同意, 现将此信附于后.

王元先生给译者的信

鸣伟教授:

非常感谢你让我预先看一看你关于韦伊的数论史名著《数论》的译稿. 很多年前, 我就想拜读这本书. 但由于该书涉及广泛, 我必须不停地查字典才能阅读而作罢. 这次有幸读你的译稿, 完了我多年的心愿.

你要我写点东西, 我不能. 我像一个对佛经一知半解的僧人见到了佛祖, 诚惶诚恐, 还能说什么呢? 书中叙述的几个数论奠基人, 早就是我崇拜的偶像. 我始终对他们怀着无限的感恩之心, 感谢他们缔造了无比优美的"数学的皇后"——数论这个纯数学的核心领域, 使我有幸终身学习她, 感受她的优美. 我应该永远怀念与感谢这几位数论的创始人.

韦伊是二十世纪最伟大的数学家之一. 这本书是他的力作. 凡弄清楚了的地方, 必将证据摆明, 有疑问及不清楚的地方, 则明确指出, 还以附录形式, 用现代的数学语言将要点再加解释. 他的这种治学态度无疑是非常宝贵的. 由于时间紧迫, 我只匆匆拜读了一遍. 正式出版后, 我还是要多次详细拜读的.

有些错排及笔误, 我用铅笔勾出, 不知妥否, 谨供参考.

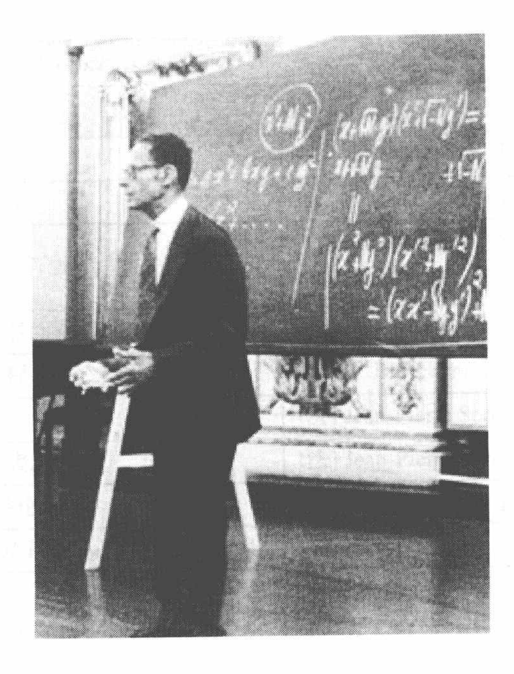
祝安好!

王元

2009 年 9 月 29 日

人名索引

内容索引



韦伊 (André Weil) 被认为是二十世纪顶尖数学家之一, 他在 1999 年逝世前是普林斯顿高等研究院的荣誉退休教授, 因其在数论和代数几何方面的工作而著名. 他对数学史毕生的兴趣浓缩地反映在这本书里, 本书是由他在高等研究院和其他一些地方的演讲汇集而成的.

“这是一本罗曼蒂克式的文献小说！它将完全的哲学准确性、敏锐的观察力、对本质问题的切题评议、生动的想象、对学科的热爱、富于才气的文学风格完美结合起来。它是数论及其历史的一个不可分割的整体，帮助我们了解这个学科最初根植于何处，以及其发展的第一个重要阶段。作为最卓越数论学家之一的作者……向我们展示了现代数论诞生的壮阔全景。”

——*Periodica Mathematica Hungaria*（匈牙利数学期刊）

“所评论的这本书……是站在许多伟大数论作者肩膀上的，对数论所作的推论性、诠释性的轻松一瞥……在激发学习数论的热情方面，或许是独特的。”

——*Mathematical Reviews*（数学评论）

数论——或者一些人称之为的算术，是最古老、最纯粹、最有活力、最初等却也是最深奥的数学领域。这门学科具有“数学皇后”的名声绝非偶然。一些最为复杂的传统的数学思想便是由对数论的基本问题的研究发展起来的。

对数论有杰出贡献的韦伊，写成了诠释数论历史的这本书；他的研究内容涵盖了大约三十六个世纪的算术工作——从一块可追溯到汉穆拉比王朝的古巴比伦的泥板到勒让德的《论数论》（1798）。韦伊一直希望向有较好教育背景的读者讲述他的研究领域，这促使他在问题的分析、数论方法的演变以及它们在数学中的意义方面使用了历史性的解读方法。在他的论述过程中，韦伊和读者一起来到现代数论的四位主要作者（费马、欧拉、拉格朗日、勒让德）的工作室，并在那里进行了一场仔细的、带有批判眼光的查验。本书富含知识史的广博内容，对了解我们的文化遗产有很重要的贡献。

学科类别：数学史

academic.hep.com.cn



定价 56.00 元